Sebastián Castañeda Hernández
Ismael Gutiérrez García

Anillos y cuerpos

UNIVERSIDAD DEL NORTE
Editorial

ANILLOS Y CUERPOS

ANILLOS Y CUERPOS

Sebastián Castañeda Hernández
Ismael Gutiérrez García

Área metropolitana
de Barranquilla (Colombia), 2019

UNIVERSIDAD DEL NORTE
Editorial

Castañeda Hernández, Sebastián.
Anillos y cuerpos / Sebastián Castañeda Hernández, Ismael Gutiérrez García. – Barranquilla, Colombia: Editorial Universidad del Norte, 2019.

205 p. 28 cm
Incluye referencias bibliográficas (p. 201-202) e índice.
ISBN 978-958-789-098-3 (PDF)

1. Anillos (Álgebra). 2. Álgebra. 3. Polinomios I. Gutiérrez García, Ismael. II. Tít.

(512.4 C346 ed. 23) (CO-BrUNB)

UNIVERSIDAD DEL NORTE
Vigilada Mineducación
www.uninorte.edu.co
Km 5, vía a Puerto Colombia, A.A. 1569
Área metropolitana de Barranquilla (Colombia)

© Universidad del Norte, 2018
Sebastián Castañeda Hernández y Ismael Gutiérrez García

Coordinación editoral
Zoila Sotomayor O.

Diseño y diagramación
Ismael Gutiérrez García

Procesos técnicos
Munir Kharfan de los Reyes

Corrección de textos
Henry Stein

Diseño de portada
Joaquín Camargo Valle

Hecho en Colombia
Made in Colombia

© Reservados todos los derechos. Queda prohibida la reproducción total o parcial de esta obra por cualquier medio reprográfico, fónico o informático, así como su transmisión por cualquier medio mecánico o electrónico, fotocopias, microfilm, *offset*, mimeográfico u otros sin autorización previa y escrita de los titulares del *copyright*. La violación de dichos derechos constituye un delito contra la propiedad intelectual.

A Elena y Matthias

LOS AUTORES

Ismael Gutierrez García

Doctor en Ciencias Naturales de la Universidad Johannes Gutenberg de Mainz (Alemania). Magíster en Matemáticas de la Universidad del Valle (Colombia) y licenciado en Matemáticas y Física de la Universidad del Atlántico (Colombia). Está vinculado a la Universidad del Norte (Colombia) como profesor titular del departamento de Matemáticas y Estadística. Posee una amplia experiencia como docente universitario y además ha liderado proyectos de investigación en el área de matemáticas discretas y sus aplicaciones, concretamente en teoría clásica de códigos y en códigos de subespacios. Es autor del libro *Matemáticas para informática*, y coautor de *Álgebra lineal* y *Matemáticas básicas con trigonometría*.

Sebastián Castañeda Hernández

Magíster en Ciencias matemáticas de la Universidad del Valle, en convenio con la Universidad del Norte (Colombia). Licenciado en Matemáticas de la Universidad del Atlántico (Colombia). Es profesor del departamento de Matemáticas y Estadística de la Universidad del Norte (Colombia) desde 1988. Es autor de los libros *Matemáticas fundamentales para estudiantes de ciencias* y *Curso básico de teoría de números*, y coautor del *Manual de álgebra lineal*.

ÍNDICE GENERAL

Prólogo **xi**

PARTE I: `Anillos`

1 Generalidades sobre anillos **xiii**

1

1.1 Definiciones y propiedades básicas 1

1.2 Subanillos, ideales y anillo cociente 16

1.3 Algunos tipos de anillos 23

2 Homomorfismos de anillos **31**

2.1 Definiciones básicas, núcleo e imagen 31

2.2 Teoremas de isomorfía 36

2.3 El cuerpo cociente de un dominio entero 40

2.4 Ejercicios 44

3 Otras propiedades de los ideales **45**

3.1 Ideales maximales e ideales primos 45

3.2 Nilpotencia 49
3.3 Ejercicios 50

4 Anillos conmutativos **53**
4.1 Divisibilidad, elementos primos y elementos irreducibles 53
4.2 Anillos de factorización única 61
4.3 Polinomios sobre anillos de factorización única 64
4.4 Ejercicios 69

PARTE II: `Cuerpos`

5 Extensiones de cuerpos **81**
5.1 Preliminares 81
5.2 Extensiones algebraicas 90
5.3 La clausura algebraica 100
5.4 Cuerpos de descomposición 112
5.5 Extensiones normales 117
5.6 Extensiones separables 120
5.7 El teorema fundamental de la teoría de Galois 131
5.8 Ejercicios 148

6 Introducción a los cuerpos finitos **155**
6.1 Preliminares 156
6.2 Existencia y unicidad de los cuerpos finitos 158
6.3 Extensiones de cuerpos finitos y automorfismos 161

7 Construcción con regla y compás **165**
7.1 Introducción 165
7.2 Elementos construibles 166
7.3 Estructura de cuerpo de $C(M)$ 172

7.4 Los tres problemas clásicos 183
7.5 Ejercicios 184

A El anillo de polinomios **185**
A.1 Polinomios en una indeterminada 185
A.2 La propiedad universal 193
A.3 Polinomios en varias indeterminadas 195

Bibliografía **201**

Índice alfabético **203**

PRÓLOGO

En el presente texto, diseñado inicialmente para estudiantes no graduados en Matemáticas, se consideran dos partes importantes del álgebra: una introducción a los resultados básicos de la teoría de anillos y los primeros elementos de la teoría de extensiones de cuerpos con característica cero o característica prima.

En el primer capítulo se presenta la definición de anillo y un gran número de ejemplos inspirados en el álgebra lineal, el cálculo diferencial y la teoría de grupos. Seguidamente se consideran subestructuras especiales: los subanillos y los ideales. Estos últimos juegan el mismo papel que los subgrupos normales, son los necesarios para construir la estructura cociente de un anillo. Posteriormente se presentan unos resultados elementales sobre anillos de ideales principales, anillos noetherianos y anillos euclidianos.

El segundo capítulo está dedicado a funciones entre anillos que preservan la estructura: los homomorfismos de anillos. Los resultados relevantes que se presentan son los tres teoremas de isomorfía y la construcción del cuerpo cociente de un dominio entero, con la conocida propiedad universal.

En el capítulo tres se presentan definiciones y caracterizaciones de ideales maximales e ideales primos. Especialmente se indagan condiciones que permitan establecer relaciones entre estos. Seguidamente consideramos el concepto de elemento e ideal nilpotente. Nuevamente se consideran ejemplos importantes para fijar los diferentes resultados.

El cuarto y último capítulo de esta primera parte está dedicado al estudio de cier-tas propiedades de los anillos conmutativos. Concretamente se presentan resultados sobre divisibilidad, elementos primos y elementos irreducibles y las relaciones entre estos conceptos. Luego presentamos los anillos de factorización única y el anillo de polinomios con coeficientes en esta clase de anillos.

El segundo tema de este libro lo constituyen las extensiones de cuerpos. En el capítulo quinto se muestran resultados básicos sobre extensiones, por ejemplo, la fórmula del grado. Seguidamente se describen la extensiones algebraicas y se demuestra la existencia y unicidad de la clausura algebraica de un cuerpo. Posteriormente se presenta el cuerpo de descomposición de un polinomio con coeficientes en un cuerpo, así como los resultados más importantes sobre extensiones normales, separables y de Galois. Para finalizar este capítulo se demuestra el teorema fundamental de la teoría de Galois acompañado de un considerable número de ejemplos.

En el capítulo sexto se presenta de manera sucinta los cuerpos finitos. Esta parte está inspirada en la necesidad de este tipo de estructuras para el estudio de estructuras discretas, y en especial la teoría de códigos de bloques o códigos con la métrica del rango.

El capítulo final del libro está dedicado a la construcción con regla y compás y especialmente a presentar tres problemas clásicos: la duplicación del cubo, la cuadratura del círculo y la trisección de un ángulo. Al final del texto se presenta un pequeño anexo sobre el anillo de los polinomios en una indeterminada.

De antemano damos gracias a los lectores por cualquier sugerencia que conduzca a mejorar la presente propuesta, la cual es fruto de los cursos dictados por los autores a lo largo de los últimos diez años, tanto en la carrera de Matemáticas como en la maestría en Matemáticas de la Universidad del Norte.

Parte I

Anillos

CAPÍTULO 1

GENERALIDADES SOBRE ANILLOS

1.1 Definiciones y propiedades básicas

1.1.1 Definición. Un conjunto no vacío R sobre el cual están definidas dos operaciones binarias " $+$ " (suma) y " $\cdot$ " (multiplicación) se denomina un `anillo` si se satisfacen las siguientes propiedades:

(1) Para todo $x, y, z \in R \;\; x + (y + z) = (x + y) + z$.

(2) Existe un elemento $0 \in R$ tal que para todo $x \in R \;\; 0 + x = x$.

(3) Para todo $x \in R$ existe $y \in R$ tal que $y + x = 0$.

(4) Para todo $x, y \in R \;\; x + y = y + x$.

(5) Para todo $x, y, z \in R \;\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(6) Para todo $x, y, z \in R \;\; x(y + z) = xy + xz$ y $(y + z)x = yx + zx$.

1.1.2 Observaciones. Los axiomas del (1) al (4) de la definición anterior indican que $(R, +)$ es un grupo abeliano con elemento neutro 0_R o simplemente 0, si no hay lugar a confusión (llamado `cero` o elemento `nulo` de R), el axioma (5) dice que $(R, \cdot)$ es un semigrupo. Si R admite un elemento neutro para la multiplicación (un uno), entonces $(R, \cdot)$ es un semigrupo con `elemento identidad` o simplemente un semigrupo con `uno` y finalmente el axioma (6) establece que la multiplicación distribuye con respecto a la adición. En adelante, en lugar de $x \cdot y$ escribimos simplemente xy.

1.1.3 Observaciones. Sea R un anillo. Escribimos $-x$ para referirnos al único inverso de un elemento x en el grupo aditivo de R. Si R tiene elemento identidad, entonces este se nota con 1_R o simplemente con 1. Si un elemento $x \in R$ es invertible multiplicativamente notaremos por x^{-1} a su único inverso.

1.1.4 Definición. Sea R un anillo.

(1) Decimos que R es `conmutativo` si para todo $x, y \in R$ se verifica que $x \cdot y = y \cdot x$.

(2) $0 \neq a \in R$ se denomina un `divisor de cero` si existe $0 \neq b \in R$ tal que $ab = 0$ o $ba = 0$.

(3) Si R es conmutativo y no tiene divisores de cero, entonces R se llama un `dominio entero`.

(4) $a \in R$ se llama `invertible`, o una `unidad` si existe $b \in R$ tal que $ab = ba = 1$. El conjunto de todas las unidades de R lo notamos con $U(R)$ o también con $R^\times$.

(5) Si todo elemento no nulo de R es invertible, entonces se dice que R es un `anillo con división`. Claramente, si R es un anillo con división, entonces $|R|$, la cardinalidad de R, es mayor o igual a dos.

(6) Si R es un anillo conmutativo con división, entonces R se denomina un `cuerpo` o un `campo`.

1.1.5 Observación. Si R es una anillo con identidad y tiene al menos dos elementos, claramente $1 \neq 0$ ya que si $1 = 0$ se tendría para todo $x \in R$ que

$$x = x1 = x0 = 0$$

lo que implicaría que $R = \{0\}$.

1.1.6 Ejemplo. Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$ (p primo) con las sumas y multiplicaciones usuales son anillos conmutativos. En particular $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$ son cuerpos.

1.1.7 Ejemplo. Sean $n \in \mathbb{N}$ con $n \geq 2$ y R un anillo. El conjunto de todas las matrices de tamaño $n \times n$ con entradas en R es un anillo no conmutativo. Este es denotado en lo que sigue con $\mathrm{Mat}(n, R)$. En particular, en $\mathrm{Mat}(n, \mathbb{R})$ existen divisores de cero. Consideremos por ejemplo:

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note que $a \neq 0$ y $b \neq 0$ y, sin embargo, $ab = 0$.

1.1.8 Ejemplo. Sea $n \in \mathbb{N}$. El conjunto $\mathbb{Z}_n$ de las clases residuales módulo n con las operaciones usuales es un anillo conmutativo. Si $n = ab$ con $a, b \neq 1$, entonces $\mathbb{Z}_n$ no es un dominio entero, ya que $[a][b] = [n] = [0]$, sin embargo $[a] \neq [0]$ y $[b] \neq [0]$.

1.1.9 Ejemplo. Si $(G, +)$ es un grupo abeliano, entonces $\mathrm{End}(G)$ es un grupo abeliano con respecto a la suma definida por:

$$(\alpha + \beta)(g) := \alpha(g) + \beta(g),$$

para todo $g \in G$. Si consideramos sobre $\mathrm{End}(G)$ la composición de funciones como la multiplicación, se verifica que $\mathrm{End}(G)$ es un anillo.

1.1.10 Ejemplo. Sean $X \neq \varnothing$ y R un anillo. El conjunto $\mathrm{Fun}(X, R)$ de todas las funciones $f : X \longrightarrow R$ con las operaciones usuales (puntuales)

$$(f + g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x),$$

para todo $f, g \in \mathrm{Fun}(X, R)$ y todo $x \in X$, es un anillo. Si R es conmutativo, entonces $\mathrm{Fun}(X, R)$ también lo es.

Como caso particular, $R = \mathrm{Fun}([a, b], \mathbb{R})$ es un anillo conmutativo con elemento identidad $f(x) = 1$ para todo $x \in [a, b]$. R no es un dominio entero. En efecto, consideremos las funciones no nulas

$$f(x) = \begin{cases} \frac{1}{2} - x, & \text{si } 0 \leq x < \frac{1}{2} \\ 0, & \text{si } \frac{1}{2} \leq x \leq 1 \end{cases}$$

$$g(x) = \begin{cases} 0, & \text{si } 0 \leq x < \frac{1}{2} \\ x - \frac{1}{2}, & \text{si } \frac{1}{2} \leq x \leq 1 \end{cases}$$

Note que $f(x)g(x) = 0$, $\forall x \in [0, 1]$ y ni f ni g son la función nula.

1.1.11 Ejemplo. El conjunto $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$ con las operaciones usuales entre números complejos es un anillo conmutativo, denominado el anillo de los `números Gaussianos`. Es claro que $\mathbb{Z}[\mathrm{i}]$ es conmutativo y sin divisores de cero. No obstante, note que

$$(1 - \mathrm{i})^{-1} = \tfrac{1}{2} + \tfrac{1}{2}\mathrm{i} \notin \mathbb{Z}[\mathrm{i}].$$

Por lo tanto, $\mathbb{Z}[\mathrm{i}]$ no es un cuerpo.

1.1.12 Ejemplo. Si $R_1, \ldots, R_n$ son anillos, entonces el producto cartesiano

$$R := R_1 \times \cdots \times R_n$$

también lo es con respecto a las siguientes operaciones:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n)$$

y

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_n b_n).$$

1.1.13 Ejemplo. Sea R un anillo y notemos con $R[[x]]$ el conjunto de todas las `series de potencias` en la indeterminada x con coeficientes en R. Esto es:

$$R[[x]] := \left\{ \sum_{j=0}^{\infty} c_j x^j \mid c_j \in R \right\}.$$

Para dos series de potencias $f = \sum_{j=0}^{\infty} a_j x^j$ y $g = \sum_{j=0}^{\infty} b_j x^j$ definimos

$$f = g \Leftrightarrow a_j = b_j, \quad \forall j \in \mathbb{N}_0$$
$$f + g = \sum_{j=0}^{\infty} (a_j + b_j) x^j$$
$$f \cdot g = \sum_{j=0}^{\infty} \Big(\sum_{i+k=j} a_i b_k \Big) x^j.$$

Se deja como ejercicio verificar que $R[[x]]$ es un anillo. Si R es conmutativo, entonces $R[[x]]$ también lo es.

1.1.14 Ejemplo. Sea R un anillo y notemos con $R[x]$ el conjunto de todos los `polinomios` en la indeterminada x con coeficientes en R. Esto es:

$$R[x] := \left\{ \sum_{j=0}^{m} c_j x^j \mid m \in \mathbb{N}_0,\ c_j \in R \right\}.$$

Para dos polinomios $f = \sum_{j=0}^{m} a_j x^j$ y $g = \sum_{j=0}^{n} b_j x^j$ definimos

$$f = g \Leftrightarrow m = n \ \wedge \ a_j = b_j, \quad \forall j$$
$$f + g = \sum_{j=0}^{\max\{m,n\}} (a_j + b_j) x^j$$
$$f \cdot g = \sum_{j=0}^{mn} \Big(\sum_{i+k=j} a_i b_k \Big) x^j.$$

Se deja como ejercicio verificar que $R[x]$ es un anillo. Si R es conmutativo, entonces $R[x]$ también lo es.

1.1.15 Ejemplo. (`Los cuaterniones de Hamilton`) Sea $\mathbb{H} \subseteq \mathrm{Mat}(2,\mathbb{C})$ definido por

$$\mathbb{H} := \left\{ \begin{pmatrix} z & -\overline{w} \\ w & \overline{z} \end{pmatrix} \middle| \; z, w \in \mathbb{C} \right\},$$

donde $\overline{z}$ y $\overline{w}$ denotan respectivamente los complejos conjugados de z y w. Si $z = a + b\mathrm{i}$ y $w = c + d\mathrm{i}$ con $a, b, c, d \in \mathbb{R}$, entonces

$$\begin{pmatrix} z & -\overline{w} \\ w & \overline{z} \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} + c \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

Si definimos

$$1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \imath := \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix},\ \jmath := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ k := \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},$$

entonces cada elemento de $\mathbb{H}$ puede expresarse en la forma

$$a1 + b\imath + c\jmath + dk,$$

con $a, b, c, d \in \mathbb{R}$. Se puede verificar sin dificultades los resultados de la siguiente tabla,

$\cdot$	1	$\imath$	$\jmath$	k
1	1	$\imath$	$\jmath$	k
$\imath$	$\imath$	-1	k	$-\jmath$
$\jmath$	$\jmath$	$-k$	-1	$\imath$
k	k	$\jmath$	$-\imath$	-1

en la cual se puede también observar que $\mathbb{H}$ es un anillo no conmutativo. Por otro lado, si para $z = a1 + b\imath + c\jmath + dk$, definimos $\overline{z} = a1 - b\imath - c\jmath - dk$, entonces se tiene que

$$z\overline{z} = \overline{z}z = (a^2 + b^2 + c^2 + d^2) \cdot 1.$$

En consecuencia, si $z \neq 0$, se tiene que

$$z^{-1} = \frac{\overline{z}}{z\overline{z}}.$$

Por lo tanto, $\mathbb{H}$ es un anillo con división, no conmutativo.

1.1.16 Ejemplos. Algunas unidades.

(1) $U(\mathbb{Z}) = \{1, -1\}$,

(2) $U(\mathbb{Z}_6) = \{[1], [5]\}$,

(3) $U(\mathbb{Z}_7) = \{[1],[2],[3],[4],[5],[6]\}$,

(4) Si $R = \mathrm{Mat}(n,K)$, entonces $U(R) = \mathrm{GL}(n,K)$.

El siguiente teorema presenta algunos resultados básicos sobre anillos. Como es usual, al decir que R es un anillo nos referimos no solamente al conjunto, sino a la estructura formada por el conjunto y las dos operaciones.

1.1.17 Teorema. Sea R un anillo.

(1) Para todo $x \in R$ se tiene $x0_R = 0_R x = 0_R$.

(2) Si $x, y \in R$, entonces:

$$-(-x) = x \tag{1.1}$$
$$-(x+y) = -x + (-y) \tag{1.2}$$
$$x(-y) = (-x)y = -(xy) \tag{1.3}$$
$$(-x)(-y) = xy \tag{1.4}$$

Demostración. (1) Se deja como ejercicio.

(2) Las propiedades (1.1) y (1.2) son casos particulares de

$$(x^{-1})^{-1} = x \quad \text{y} \quad (xy)^{-1} = y^{-1}x^{-1},$$

las cuales son válidas en un monoide para elementos invertibles, x e y. En particular, son válidas para la estructura multiplicativa de un anillo con identidad y elementos no singulares x, y (ver, por ejemplo, [3], teorema 2.1.1, página 50). □

De igual manera se tiene que $U(R)$, el conjunto de las unidades en un anillo con identidad, es un grupo multiplicativo, ya que en todo monoide el conjunto de los elementos invertibles lo es.

Similar como en los grupos, si R es un anillo podemos definir potencias enteras nx de un elemento x en el grupo aditivo $(R,+)$.

1.1.18 Definición. Sean R un anillo, $x \in R$ y $n \in \mathbb{Z}$. Definimos

$$nx = \begin{cases} 0_R, & \text{si } n = 0; \\ (n-1)x + x, & \text{si } n > 0; \\ -((-n)x), & \text{si } n < 0. \end{cases} \tag{1.5}$$

La notación x^n se utiliza para potencias multiplicativas con $n > 0$. Así tenemos

$$x^n = \begin{cases} x & \text{si } n = 1; \\ x^{n-1}x, & \text{si } n > 1. \end{cases} \tag{1.6}$$

Las propiedades de la potenciación entera en grupos y en grupos abelianos adoptan entonces las siguientes formas específicas en la estructura aditiva de grupo abeliano de un anillo R.

1.1.19 Teorema. Sean R un anillo, $x, y \in R$ y $n, m \in \mathbb{Z}$. Entonces:

$$m(nx) = (mn)x = n(mx) \tag{1.7}$$
$$mx + nx = (n+m)x \tag{1.8}$$
$$n(x+y) = nx + ny \tag{1.9}$$
$$(nx)y = x(ny) = n(xy) \tag{1.10}$$
$$(nx)(my) = (nm)(xy) \tag{1.11}$$

Demostración. Es claro que (1.11) es consecuencia de (1.10). Demostremos esta última inicialmente para $n \geq 0$, utilizando inducción.

El caso $n = 0$ es trivial. Supongamos entonces que los resultados son válidos para un cardinal n. Tenemos entonces:

$$\begin{aligned} ((n+1)x)y &= (nx+x)y \\ &= (nx)y + (xy) \\ &= n(xy) + (xy) \\ &= (n+1)(xy). \end{aligned}$$

También

$$\begin{aligned} ((n+1)x)y &= (nx)y + (xy) \\ &= x(ny) + xy \\ &= x(ny+y) \\ &= x((n+1)y), \end{aligned}$$

lo que concluye la demostración para el caso $n \geq 0$. Si $n < 0$, tenemos

$$\begin{aligned} (nx)y &= (-((-n)x))y \\ &= -(((-n)x)y) \\ &= -(x((-n)y)) \\ &= x(-((-n)y)) \\ &= x(ny). \end{aligned}$$

De manera similar, para el caso $n < 0$, se demuestra $(nx)y = n(xy)$.

El resto se deja como ejercicio. □

Para anillos conmutativos con identidad tenemos una extensión del conocido teorema del binomio; sin embargo, una hipótesis más general requiere solo que dos elementos del anillo conmuten bajo la multiplicación. Antes, recordamos la definición del coeficiente binomial.

1.1.20 Definición. Sean $n \in \mathbb{N}_0$ y $j \in \mathbb{Z}$. Definimos el `coeficiente binomial` de n con j de la siguiente manera:

$$\binom{n}{j} = \begin{cases} \dfrac{n!}{j!(n-j)!} & \text{si } 0 \leq j \leq n \\ 0 & \text{en otro caso.} \end{cases}$$

Es razonable asignar el valor de cero al coeficiente binomial cuando $j < 0$ o $j > n$, ya que en estos casos carece de sentido seleccionar menos de cero o más de n objetos de un conjunto con n elementos.

1.1.21 Lema. Sean $n \in \mathbb{N}_0$ y $j \in \mathbb{Z}$. Entonces

(1) (`Simetría`) $\binom{n}{j} = \binom{n}{n-j}$.

(2) (`Adición`) $\binom{n+1}{j} = \binom{n}{j} + \binom{n}{j-1}$.

Demostración. Se deja como ejercicio. □

1.1.22 Teorema. (Binomio) Sea R un anillo, $a, b \in R$ con $ab = ba$ y $n \in \mathbb{N}_0$. Entonces,

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j.$$

Demostración. Procedemos por inducción sobre n.

Si $n = 0$, entonces la afirmación se cumple inmediatamente.

Supongamos que la afirmación es válida para $n \geq 0$. Entonces,

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b) \\
&= \Big(\sum_{j=0}^{n} \tbinom{n}{j} a^{n-j}b^j\Big)(a+b) \\
&= \Big(\sum_{j=0}^{n} \tbinom{n}{j} a^{n-j}b^j\Big)a + \Big(\sum_{j=0}^{n} \tbinom{n}{j} a^{n-j}b^j\Big)b \\
&= \sum_{j=0}^{n} \tbinom{n}{j} a^{(n+1)-j}b^j + \sum_{j=0}^{n} \tbinom{n}{j} a^{n-j}b^{j+1} \\
&= \sum_{j=1}^{n} \tbinom{n}{j} a^{(n+1)-j}b^j + a^{n+1} + \sum_{j=0}^{n-1} \tbinom{n}{j} a^{n-j}b^{j+1} + b^{n+1} \\
&= a^{n+1} + \sum_{j=1}^{n} \tbinom{n}{j} a^{(n+1)-j}b^j + \sum_{j=1}^{n} \tbinom{n}{j-1} a^{n-(j-1)}b^{(j-1)+1} + b^{n+1} \\
&= a^{n+1} + \sum_{j=1}^{n} \tbinom{n}{j} a^{(n+1)-j}b^j + \sum_{j=1}^{n} \tbinom{n}{j-1} a^{(n+1)-j}b^j + b^{n+1} \\
&= a^{n+1} + \sum_{j=1}^{n} \Big(\tbinom{n}{j} + \tbinom{n}{j-1}\Big) a^{(n+1)-j}b^j + b^{n+1} \\
&= a^{n+1} + \sum_{j=1}^{n} \tbinom{n+1}{j} a^{(n+1)-j}b^j + b^{n+1} \\
&= \sum_{j=0}^{n+1} \tbinom{n+1}{j} a^{(n+1)-j}b^j.
\end{aligned}$$

Para obtener la última igualdad hemos utilizado

$$\tbinom{n+1}{0} a^{(n+1)-0}b^0 = a^{n+1} \quad \text{y} \quad \tbinom{n+1}{n+1} a^{(n+1)-(n+1)}b^{n+1} = b^{n+1}.$$

1.1.23 Observación. En un anillo R, sin divisores de cero, claramente se cumple que dados $a, b \in R$, entonces:

$$ab = 0_R \iff a = 0_R \vee b = 0_R. \tag{1.12}$$

En particular, elementos no nulos son `cancelables`; es decir, si $a \neq 0_R$, entonces si $ab = ac$ o $ba = ca$ se sigue necesariamente que $b = c$. Es claro que todo cuerpo es un dominio entero (ejercicio). El recíproco es, en general, falso como lo muestra el ejemplo del anillo de los enteros, el cual es un dominio entero pero no es un cuerpo, ya que sus únicas unidades son 1 y -1. Sin embargo, en el caso particular en que el dominio entero sea finito se tiene entonces un cuerpo.

1.1.24 Teorema. Sea $D = \{x_1, x_2, \ldots, x_n\}$ con $n \geq 2$, un anillo conmutativo sin divisores de cero. Entonces, D es un cuerpo.

DEMOSTRACIÓN. Puesto que $n \geq 2$ existe al menos un elemento $x_i \neq 0_D$. Ahora, para $1 \leq j < l \leq n$, si $x_i x_j = x_i x_l$ se tendría $x_j = x_l$. Así que los n productos $x_i x_j = x_j x_i$, $j = 1, \ldots, n$, son todos distintos.
Por lo tanto, existe un $x_{i'}$ tal que $x_i x_{i'} = x_{i'} x_i = x_i$. Mostremos que $x_{i'}$ es elemento identidad de D.
Tenemos que para cada $j \in \{1, 2, \ldots, n\}$ existe j' tal que $x_j = x_i x_{j'}$ y se tiene

$$\begin{aligned} x_j x_{i'} &= x_{i'} x_j \\ &= x_{i'}(x_i x_{j'}) \\ &= (x_{i'} x_i) x_{j'} \\ &= x_i x_{j'} \\ &= x_j, \end{aligned}$$

por lo que $x_{i'} = 1_D$. De manera similar, para un elemento $x_j \neq 0_D$, todos los productos $x_j x_k$ con $k = 1, \ldots, n$ son distintos y, por lo tanto, existe l tal que $x_j x_l = 1_D$; es decir $x_l = x_j^{-1}$.

La característica de un anillo

1.1.25 Definición. Dado un anillo R, decimos que R tiene `característica cero` si para todo entero positivo n existe $x \in R$ tal que $nx \neq 0$. Si R no tiene característica cero, entonces existe al menos un entero positivo n tal que para todo $x \in R$ se tiene $nx = 0$. En tal caso, el mínimo entero positivo con tal propiedad es la `característica` de R. Escribimos $\text{char}(R)$ para referirnos a la característica del anillo R.

1.1.26 Ejemplos. El anillo de los números enteros tiene característica cero pues, dado $n \in \mathbb{Z}^+$ se tiene que $n1 = n \neq 0$. De igual manera, el anillo de los racionales (reales, complejos, respectivamente) es un anillo de característica cero. Por su parte, el anillo $(\mathbb{Z}_n, +, \cdot)$ es de característica n.

1.1.27 Teorema. Sea R un anillo con elemento identidad. Si $n = \text{char}(R) > 0$, n es el menor entero positivo para el cual $n1 = 0$. Si, además, R es dominio entero (con identidad), entonces n es un número primo.

DEMOSTRACIÓN. Si $m1 = 0$ para un entero positivo m, entonces para todo $x \in R$ se tiene $mx = m(1x) = (m1)x = 0$, por lo que $m \geq n$.

Supongamos que se tienen enteros positivos p, q tales que $n = pq$, entonces

$$(p1)(q1) = (pq)1 = n1 = 0.$$

Si R es dominio entero se sigue que $p1 = 0$ o $q1 = 0$, de donde $p \geq n$ o $q \geq n$. Se tiene entonces que uno de los dos (p o q) es n y el otro es 1. Así, n es primo. □

En particular, el teorema anterior nos dice que la característica de un cuerpo es cero o un número primo.

1.1.28 Definición. Sean K un cuerpo y A un conjunto no vacío sobre el cual están definidas dos operaciones binarias " $+$ " (suma) y " $*$ " (multiplicación) y, además, una multiplicación por escalar " $\cdot$ ". Decimos que A es un `álgebra` sobre K o simplemente una K-`álgebra` si se verifican:

(1) $(A, +, \cdot)$ es un espacio vectorial de dimensión finita sobre K.

(2) $(A, +, *)$ es un anillo.

(3) $u * (k \cdot v) = (k \cdot u) * v = k \cdot (u * v)$ para todo $u, v \in A$ y todo $k \in K$.

(4) Existe un elemento $1 \in A$, tal que $1 * a = a * 1 = a$ para todo $a \in A$.

1.1.29 Ejemplos. Sea K un cuerpo.

(1) El conjunto de las matrices cuadradas $\mathrm{Mat}(n, K)$ es una K-álgebra de dimensión n^2.

(2) Sea V un espacio vectorial de dimensión n sobre K. Si consideramos como multiplicación sobre $A := \mathrm{End}_K(V)$ la composición de funciones, entonces A es una K-álgebra de dimensión n^2.

(3) Sean $X = \{x_1, \ldots, x_n\}$ un conjunto finito. El conjunto $A := \mathrm{Fun}(X, K)$ con las operaciones usuales (puntuales)

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x) \tag{1.13}$$

$$(k \cdot \alpha)(x) = k\alpha(x) \tag{1.14}$$

$$(\alpha * \beta)(x) = \alpha(x)\beta(x), \tag{1.15}$$

para todo $\alpha, \beta \in A$, $k \in K$ y $x \in X$, es una K-álgebra de dimensión n. En efecto, para $j \in \{1, \ldots n\}$ definamos las n funciones e_j de la siguiente manera:

$$e_j(x_i) := \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

Sea ahora $B := (e_j \mid j \in \{1, \ldots n\})$. Demostramos que B es una base para A.

(1) B `genera a` A. Si $\alpha \in A$, entonces $\alpha = \sum_{j=1}^{n} a_j e_j$, donde $a_j = \alpha(x_j)$.

(2) B `es linealmente independiente.` Supongamos que

$$\sum_{j=1}^{n} a_j e_j = 0.$$

Entonces para todo $x \in X$ se verifica que

$$0 = \sum_{j=1}^{n} a_j e_j(x) = a_j.$$

1.1.30 Ejemplo. (The Group Ring) Sea $G = \{g_1, \ldots, g_n\}$ un grupo finito, notado multiplicativamente. Denotemos con KG el conjunto $\mathrm{Fun}(G, K)$ del ejemplo anterior. Usando las operaciones (1.13) y (1.14) podemos dotar a KG con la estructura de espacio vectorial sobre K. Definamos ahora sobre KG una nueva multiplicación, es decir, una diferente a la puntual dada por (1.15). La nueva multiplicación se denomina usualmente una `convolución` y está dada por:

$$(\alpha * \beta)(x) = \sum_{z \in G} \alpha(z)\beta(z^{-1}x), \tag{1.16}$$

para todo $\alpha, \beta \in KG$ y $x \in G$. O equivalentemente

$$(\alpha * \beta)(x) = \sum_{uv=x} \alpha(u)\beta(v). \tag{1.17}$$

Una base para KG está dada entonces por $B := (e_g \mid g \in G)$, donde

$$e_g(x) := \begin{cases} 1 & \text{si } g = x \\ 0 & \text{si } g \neq x. \end{cases}$$

Entonces, para $\alpha \in \mathrm{Fun}(G, K)$ se verifica que

$$\alpha = \sum_{g \in G} \alpha(g) e_g.$$

Note además que para todo $g, h \in G$ se verifica:

$$\begin{aligned} (e_g * e_h)(x) &= \sum_{y \in G} e_g(y) e_h(y^{-1}x) \\ &= e_g(g) e_h(g^{-1}x) \\ &= \begin{cases} 1 & \text{si } x = gh \\ 0 & \text{si } x \neq gh \end{cases} \\ &= e_{gh}(x). \end{aligned}$$

Es decir, $e_g * e_h = e_{gh}$.

Para simplificar la notación identificamos cada elemento e_g en la base B de KG con $g \in G$. En consecuencia, todo $\alpha \in KG$ puede escribirse en la forma

$$\alpha = \sum_{g \in G} \alpha(g) g.$$

Observe que la multiplicación en KG se hace más fácil de usar con la siguiente regla: sea $\alpha, \beta \in KG$

$$\begin{aligned}
\alpha * \beta &= \sum_{g \in G} \alpha(g) g * \sum_{h \in G} \beta(h) h \\
&= \sum_{g \in G} \sum_{h \in G} \alpha(g)\beta(h) gh \\
&= \sum_{z \in G} \Big(\sum_{g \in G} \alpha(g)\beta(g^{-1}z) \Big) z \\
&= \sum_{z \in G} \Big(\sum_{uv = z} \alpha(u)\beta(v) \Big) z.
\end{aligned}$$

Con esta nueva notación las operaciones sobre KG pueden escribirse de la siguiente manera:

$$\sum_{g \in G} \alpha(g) g + \sum_{g \in G} \beta(g) g = \sum_{g \in G} (\alpha(g) + \beta(g)) g \tag{1.18}$$

$$k\Big(\sum_{g \in G} \alpha(g) g \Big) = \sum_{g \in G} (k\alpha(g)) g \tag{1.19}$$

$$\sum_{g \in G} \alpha(g) g * \sum_{h \in G} \beta(h) h = \sum_{z \in G} \Big(\sum_{uv = z} a(u)\beta(v) \Big) z. \tag{1.20}$$

Se verifica sin dificultades que KG con estas operaciones es un K-álgebra. Demostramos a continuación que KG es un anillo.

`Asociatividad de la multiplicación.` Sean $\alpha = \sum_{g \in G} \alpha(g) g$, $\beta = \sum_{h \in G} \beta(h) h$ y $\gamma = \sum_{k \in G} \gamma(k) k \in KG$. Entonces

$$\begin{aligned}
(\alpha * \beta) * \gamma &= \sum_{u \in G} \Big(\overbrace{\sum_{gh = u} \alpha(g)\beta(h)}^{d(u)} \Big) u \cdot \sum_{k \in G} \gamma(k) k \\
&= \sum_{x \in G} \Big(\sum_{uk = x} d(u)\gamma(k) \Big) x \\
&= \sum_{x \in G} \Big(\sum_{uk = x} \sum_{gh = u} \alpha(g)\beta(h)\gamma(k) \Big) x \\
&= \sum_{x \in G} \Big(\sum_{ghk = x} \alpha(g)\beta(h)\gamma(k) \Big) x.
\end{aligned}$$

Por otro lado,

$$\begin{aligned}\alpha * (\beta * \gamma) &= \sum_{g\in G} \alpha(g)g \cdot \sum_{u\in G} \Big(\overbrace{\sum_{hk=u} \beta(h)\gamma(k)}^{l(u)} \Big) u \\ &= \sum_{x\in G} \Big(\sum_{gu=x} \alpha(g)l(u) \Big) x \\ &= \sum_{x\in G} \Big(\sum_{gu=x} \sum_{hk=u} \alpha(g)\beta(h)\gamma(k) \Big) x \\ &= \sum_{x\in G} \Big(\sum_{ghk=x} \alpha(g)\beta(h)\gamma(k) \Big) x.\end{aligned}$$

`Distributividad de la multiplicación con respecto a la suma.` Sean $\alpha = \sum_{g\in G} \alpha(g)g$, $\beta = \sum_{h\in G} \beta(h)h$ y $\gamma = \sum_{h\in G} \gamma(h)h \in KG$. Entonces

$$\begin{aligned}\alpha * (\beta + \gamma) &= \sum_{g\in G} \alpha(g)g \cdot \sum_{h\in G} (\beta(h) + \gamma(h))h \\ &= \sum_{u\in G} \Big(\sum_{gh=u} \alpha(g)(\beta(h) + \gamma(h)) \Big) u \\ &= \sum_{u\in G} \Big(\sum_{gh=u} \alpha(g)\beta(h) + \sum_{gh=u} \alpha(g)\gamma(h) \Big) u \\ &= \sum_{u\in G} \Big(\sum_{gh=u} \alpha(g)\beta(h) \Big) u + \sum_{u\in G} \Big(\sum_{gh=u} \alpha(g)\gamma(h) \Big) u \\ &= \alpha * \beta + \alpha * \gamma.\end{aligned}$$

1.1.31 Ejemplo. Sea $G = \langle x \rangle$ un grupo cíclico de orden n. Entonces

$$\begin{aligned}\mathbb{R}G &= \Big\{ \sum_{g\in G} a(g)g \mid a(g) \in \mathbb{R} \Big\} \\ &= \Big\{ \sum_{i=0}^{n-1} a(x^i)x^i \mid a(x^i) \in \mathbb{R} \Big\}.\end{aligned}$$

Si definimos $a_i := a(x^i)$, entonces los elementos de $\mathbb{R}G$ tienen la forma $\sum_{i=0}^{n-1} a_i x^i$ y la multiplicación se transforma en

$$\sum_{i=0}^{n-1} a_i x^i \cdot \sum_{j=0}^{n-1} b_j x^j = \sum_{k=0}^{n-1} \Big(\sum_{i+j=k \bmod n} a_i b_j \Big) x^k.$$

Es decir,

$$\mathbb{R}G \cong \mathbb{R}[x]/\langle x^n - 1 \rangle.$$

1.1.32 Ejemplo. Sea $G = \langle x \rangle = \{x, e\}$ el grupo cíclico de orden 2, usualmente notado con C_2 y sea K el cuerpo binario $\mathbb{F}_2$. Entonces

$$\begin{aligned}\mathbb{F}_2C_2 &= \Big\{ \sum_{g\in G} a(g)g \mid a(g) \in \mathbb{F}_2 \Big\} \\ &= \{ae + bx \mid a, b \in \mathbb{F}_2\} \\ &= \{0e + 0x, 1e + 0x, 0e + 1x, 1e + 1x\}.\end{aligned}$$

Si definimos $\alpha := 0e + 1x$, entonces

$$\mathbb{F}_2C_2 = \{0, 1, \alpha, 1 + \alpha\}.$$

Note que

$$1 + 1 = 1e + 1e = (1 + 1)e = 0e = 0.$$

$$\alpha + \alpha = 1x + 1x = (1 + 1)x = 0x = 0.$$

$$(1 + \alpha) + (1 + \alpha) = \alpha + \alpha = 0.$$

Entonces tenemos:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Para tener la tabla de la multiplicación es suficiente el siguiente cálculo:

$$(1 + \alpha) \cdot (1 + \alpha) = 1 + \alpha + \alpha + \alpha^2 = 0.$$

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	1	$1+\alpha$
$1+\alpha$	0	$1+\alpha$	$1+\alpha$	0

1.1.33 Observación. El anillo $\mathbb{F}_2C_2$ tiene 4 elementos. Se puede observar de la tabla que la estructura aditiva es isomorfa a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Es decir, $(\mathbb{F}_2C_2, +)$ corresponde al 4-grupo de Klein. En consecuencia, $\mathbb{F}_2C_2$ es un anillo con 4 elementos no isomorfo, como anillo, a $\mathbb{Z}_4$.

1.1.34 Lema. Sean K una cuerpo finito y G un grupo finito. Entonces KG es una anillo finito con orden $|K|^{|G|}$.

DEMOSTRACIÓN. Es una consecuencia inmediata de la contrucción de KG. □

1.1.35 Ejemplo. Consideremos ahora el anillo $\mathbb{F}_3C_2$.

$$\begin{aligned}\mathbb{F}_3C_2 &= \Big\{ \sum_{g\in G} a(g)g \mid a(g) \in \mathbb{Z}_3 \Big\} \\ &= \{ae + bx \mid a, b \in \mathbb{Z}_3\}.\end{aligned}$$

Listamos a continuación los elementos de $\mathbb{F}_3C_2$:

$$\begin{array}{lll} 0e+0x, & 0e+1x, & 0e+2x, \\ 1e+0x, & 1e+1x, & 1e+2x \\ 2e+0x, & 2e+1x, & 2e+2x. \end{array}$$

Como en el ejemplo anterior, definamos $\alpha := 0e + 1x$. Entonces

$$\mathbb{F}_3C_2 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 2\alpha+1, 2\alpha+2\}.$$

Note que el conjunto de las unidades de $\mathbb{F}_3C_2$ está dado por:

$$U(\mathbb{F}_3C_2) = \{1, 2, \alpha, 2\alpha\},$$

mientras que el conjunto de los divisores de cero de $\mathbb{F}_3C_2$ es:

$$\{1+\alpha, 2+\alpha, 1+2\alpha, 2+2\alpha\},$$

todo esto trae como consecuencia que $\mathbb{F}_3C_2$ no es isomorfo, como anillo, a $\mathbb{Z}_9$.

1.2 Subanillos, ideales y anillo cociente

Subanillos

1.2.1 Definición. Sean R un anillo y S un subconjunto no vacío de R. Decimos que S es un `subanillo` de R si y solo si se verifican:

(1) $(S, +)$ es un subgrupo de $(R, +)$. Es decir, para todo $x, y \in S$ se verifica que $x - y \in S$.

(2) Para todo $x, y \in S$ se tiene que $xy \in S$.

1.2.2 Observación. La anterior definición de subanillo es equivalente a afirmar que al restringir las operaciones suma y multiplicación al conjunto S, entonces S es un anillo.

1.2.3 Ejemplos. (1) Si R es un anillo, entonces $\{0\}$ y R son subanillos de R, denominados subanillos `triviales`.

(2) $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ son subanillos de $\mathbb{C}$.

(3) $n\mathbb{Z}$ es un subanillo de $\mathbb{Z}$.

(4) Para todo anillo R se verifica que $R[x]$ es un subanillo de $R[[x]]$.

(5) Sea $n \in \mathbb{N}$. Los siguientes conjuntos son subanillos de $\mathrm{Mat}(n, \mathbb{R})$:

   (a) El conjunto de las matrices escalares.

   (b) El conjunto de las matrices diagonales.

   (c) El conjunto de las matrices triangulares (superiores o inferiores).

(6) Sean R un anillo y $a \in R$, fijo. Definamos

$$I(a) := \{r \in R \mid ar = 0\}.$$

Se verifica que $I(a)$ es un subanillo de R.

(7) Sean R un anillo y $a \in R$, fijo. Definamos

$$aR := \{ar \mid r \in R\}.$$

Se verifica que aR es un subanillo de R.

(8) Para todo anillo R, el `centro` de R, notado con $\mathrm{Z}(R)$ se define por

$$\mathrm{Z}(R) := \{r \in R \mid xr = rx \ \ \forall x \in R\}.$$

$Z(R)$ es un subanillo de R.

Ideales

1.2.4 Definición. Sea R un anillo e I un subgrupo de $(R, +)$.

(1) I se denomina un `ideal izquierdo` de R si para todo $x \in I$ y todo $r \in R$ se verifica que $rx \in I$.

(2) I se llama un ideal `ideal derecho` de R si para todo $x \in I$ y todo $r \in R$ se verifica que $xr \in I$.

(3) Si se verifican las dos propiedades, entonces se dice que I es un ideal `bilateral` o simplemente un `ideal` de R. Si I es un ideal de R con $I \neq R$, entonces I se llama un ideal `propio`.

1.2.5 Ejemplos. (1) Si R es un anillo, entonces $\{0\}$ y R son ideales de R, denominados ideales `triviales`. Un anillo que solo admite ideales triviales se denomina `simple`.

(2) $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ no son ideales de $\mathbb{C}$.

(3) $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$. Más aún, todo ideal de $\mathbb{Z}$ tiene esta forma.

(4) Sea R un anillo. $R[x]$ no es un ideal de $R[[x]]$.

(5) Sea $n \in \mathbb{N}$. Los siguientes conjuntos no son ideales de $\mathrm{Mat}(n, \mathbb{R})$:

   (a) El conjunto de las matrices escalares.
   (b) El conjunto de las matrices diagonales.
   (c) El conjunto de las matrices triangulares (superiores o inferiores).

   ¿Qué forma tienen los ideales de $\mathrm{Mat}(n, R)$?

(6) Sea R conmutativo y $a \in R$, fijo. Sea nuevamente

$$I(a) := \{r \in R \mid ar = 0\}.$$

   Se verifica que $I(a)$ es un ideal de R.

(7) Sea $a \in R$, fijo. Definamos

$$aR := \{ar \mid r \in R\}.$$

   Se verifica que aR es un ideal derecho de R. Si R es conmutativo, entonces aR es un ideal de R.

(8) El centro $Z(R)$ de un anillo R no necesariamente es un ideal de R.

1.2.6 Teorema. Sea R un anillo conmutativo con elemento identidad. Son equivalentes:

(1) R es un cuerpo

(2) R es simple.

Demostración. (1) $\Rightarrow$ (2). Sea $I \neq \{0\}$ un ideal de R. Entonces existe $0 \neq r \in R$. Por lo tanto, $1 = rr^{-1} \in I$. Por consiguiente, si $x \in R$, se verifica que $x = 1x \in I$ y se tiene que $I = R$.

(2) $\Rightarrow$ (1). Supongamos que R es simple. Sea $0 \neq r \in R$. Entonces $aR = R$. Por lo tanto, para $1 \in R$ existe $b \in R$ tal que $1 = ab$, lo cual demuestra que a es invertible. En consecuencia, R es un cuerpo. □

1.2.7 Teorema. Sea R un anillo con elemento identidad. Para todo $n \in \mathbb{N}$, la asignación

$$I \longmapsto \mathrm{Mat}(n, I) \tag{1.21}$$

define una biyección entre el conjunto de los ideales de R y el conjunto de los ideales de $\mathrm{Mat}(n, R)$. En particular, $\mathrm{Mat}(n, R)$ es simple si y solo si R lo es.

Demostración. Demostramos inicialmente que, dado I, un ideal de R, entonces $\mathrm{Mat}(n, I)$ es un ideal de $\mathrm{Mat}(n, R)$. Dado que $0 \in \mathrm{Mat}(n, I)$, se sigue que $\mathrm{Mat}(n, I) \neq \varnothing$. Sean ahora $A = (a_{ij})$, $B = (b_{ij}) \in \mathrm{Mat}(n, I)$. Entonces $A - B = (c_{ij})$, donde $c_{ij} = a_{ij} - b_{ij}$. Dado que I es un ideal de R, se sigue que $c_{ij} \in I$ para todo $i, j \in \{1, \ldots, n\}$. Por otro lado, para $A = (a_{ij}) \in \mathrm{Mat}(n, I)$ y $D = (d_{jk}) \in \mathrm{Mat}(n, R)$ se verifica que $AD = (f_{ik})$, donde $f_{ik} = \sum_{j=1}^{n} a_{ij} d_{jk}$. Nuevamente, dado que I es un ideal de R, se sigue que $f_{ik} \in I$ para todo $i, k \in \{1, \ldots, n\}$. En consecuencia, $AD \in \mathrm{Mat}(n, I)$. Similar se demuestra que $DA \in \mathrm{Mat}(n, I)$.

Para demostrar la inyectividad de la función (1.21), sean I, J ideales de R con $I \neq J$. Entonces existe $x \in I \setminus J$, y por lo tanto, la matriz

$$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in \mathrm{Mat}(n, I) \setminus \mathrm{Mat}(n, J).$$

Es decir, $\mathrm{Mat}(n, I) \neq \mathrm{Mat}(n, J)$.

Para demostrar la sobreyectividad de la función (1.21), sea J un ideal cualquiera de $\mathrm{Mat}(n, R)$; denotemos con I el subconjunto de R que consta de las entradas de las matrices pertenecientes a J.

Sean $a, b \in I$. Entonces existen matrices $A = (a_{ij}), B = (b_{ij}) \in J$ tales que $a = a_{kl}$ y $b = b_{rs}$ con $k, l, r, s \in \{1, \ldots, n\}$. Para $i, j \in \{1, \ldots, n\}$ notemos con $E_{ij} \in \mathrm{Mat}(n, R)$ la matriz que tiene un 1 en la entrada ij y cero en el resto de posiciones. (Estas matrices se denominan `unidades matriciales`). Consideremos ahora la matriz $C := A - E_{kr} B E_{sl}$. Es claro que $C \in J$. En consecuencia, si $C = (c_{ij})$, entonces se verifica sin dificultades que $a - b = c_{kl} \in I$.

Sea ahora $r \in R$ cualquiera. Como es usual notemos con I_n la matriz identidad de tamaño n. Entonces se verifica que $A(rI_n), (rI_n A) \in J$ y consecuentemente, $ar, ra \in I$. Con esto se ha demostrado que I es un ideal de R.

Para finalizar demostramos que $J = \mathrm{Mat}(n, I)$. De la definición de I se sigue inmediatamente que $J \subseteq \mathrm{Mat}(n, I)$. Para demostrar la otra contenencia es suficiente probar que $aE_{ij} \in J$ para todo $a \in I$ y todo $i, j \in \{1, \ldots, n\}$, ya que toda $A = (a_{ij}) \in \mathrm{Mat}(n, I)$ puede expresarse en la forma $A = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} E_{ij}$. Usando la notación de arriba se tiene que $aE_{ij} = E_{ik} A E_{lj} \in J$. □

1.2.8 Lema. Sean R un anillo y $\{I_\lambda \mid \lambda \in \Lambda\}$ un conjunto de ideales de R. Entonces $\bigcap_{\lambda\in\Lambda} I_\lambda$ es un ideal de R.

DEMOSTRACIÓN. Se deja como ejercicio. □

1.2.9 Observación. En general, $\bigcup_{\lambda\in\Lambda} I_\lambda$ no es un ideal de R.

1.2.10 Definición. Sean I, J ideales izquierdos (derechos) de un anillo R. Definimos

(1) $I + J := \{i + j \mid i \in I,\ k \in j\}$

(2) $IJ := \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I,\ b_i \in J,\ n \in \mathbb{N} \right\}$.

1.2.11 Lema. Sean I, J ideales izquierdos de R. Entonces

(1) $I + J$ es un ideal izquierdo de R.

(2) IJ es un ideal izquierdo de R.

(3) Si I, J son ideales bilaterales, entonces $IJ \subseteq I \cap J \subseteq I + J$.

DEMOSTRACIÓN. (1) Es claro que $0 \in I + J$, por lo tanto, $I + J \neq \varnothing$. Sean $i_1 + j_1, i_2 + j_2 \in I + J$ y $r \in R$. Entonces

$$(i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J.$$

Por otro lado,

$$r(i_1 + j_1) = ri_1 + rj_1 \in I + J.$$

En resumen se tiene que $I + J$ es un ideal izquierdo de R.

(2) Nuevamente se tiene que $0 \in IJ$, por lo tanto, $IJ \neq \varnothing$. Sean $r \in R$, $\sum_{i=1}^{n} a_i b_i$, $\sum_{j=1}^{m} c_j d_j \in IJ$ con $m, n \in \mathbb{N}$, $a_i, c_j \in I$ y $b_i, d_j \in J$. Si definimos

$$x_1 = a_1, \ldots, x_n = a_n,\ x_{n+1} = -c_1, \ldots, x_{n+m} = -c_m$$

y

$$y_1 = b_1, \ldots, y_n = b_n,\ y_{n+1} = d_1, \ldots, y_{n+m} = d_m,$$

entonces

$$\sum_{i=1}^{n} a_i b_i - \sum_{j=1}^{m} c_j d_j = \sum_{k=1}^{n+m} x_k y_k \in IJ.$$

Por otro lado,

$$r\Big(\sum_{i=1}^{n} a_i b_i\Big) = \sum_{i=1}^{n} (r a_i) b_i \in IJ$$

y

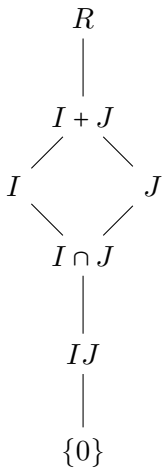
$$\Big(\sum_{i=1}^{n} a_i b_i\Big) r = \sum_{i=1}^{n} a_i (b_i r) \in IJ.$$

En resumen se tiene que IJ es un ideal de R.

(3) Sea $x = \sum_{i=1}^{n} a_i b_i \in IJ$ con $n \in \mathbb{N}$, $a_i \in I$ y $b_i \in J$. Para todo $i = 1, \ldots, n$ se verifica que $a_i b_i \in I$ y $a_i b_i \in J$. Es decir para todo $i = 1, \ldots, n$ se verifica que $a_i b_i \in I \cap J$. Por lo tanto, $x \in I \cap J$ y se tiene la primera contenencia.

Dado que $I \cap J \subseteq I \subseteq I + J$, se tiene la segunda contenencia. □

Una ilustración reticular:



1.2.12 Lema. Sean I_1, I_2, I_3 ideales izquierdos (derechos) de un anillo R. Entonces

(1) $I_1 R = R I_1 = I_1$

(2) $I_1 + (I_2 + I_3) = (I_1 + I_2) + I_3$

(3) $I_1 + I_2 = I_2 + I_1$

(4) $I_1(I_2 I_3) = (I_1 I_2) I_3$

(5) $I_1(I_2 + I_3) = I_1 I_2 + I_1 I_3$

(6) $(I_1 + I_2) I_3 = I_1 I_3 + I_2 I_3$

Demostración. Se deja como ejercicio. □

El anillo cociente

Los ideales en la teoría de anillos juegan el mismo papel de los subgrupos normales en la teoría de grupos. Si I es un ideal de un anillo R, entonces dado que el grupo aditivo es abeliano, se tiene que I es un subgrupo normal de R y puede construirse la estructura de grupo cociente R/I, teniendo como operación la suma

$$(a+I)+(b+I) := (a+b)+I. \tag{1.22}$$

El grupo abeliano $(R/I,+)$ puede dotarse de la estructura de anillo, como vemos a continuación.

1.2.13 Teorema. Sea I un ideal de un anillo R. Entonces el grupo cociente aditivo R/I adquiere la estructura de anillo con la multiplicación definida por

$$(a+I)\cdot(b+I) := ab+I. \tag{1.23}$$

Si R es un anillo conmutativo o tiene elemento identidad, entonces R/I también lo es.

Demostración. Demostramos inicialmente que la multiplicación (1.23) está bien definida. Para ello supongamos que $a+I = a'+I$ y $b+I = b'+I$ y demostramos que $ab+I = a'b'+I$. Es claro que $a-a' \in I$ y $b-b' \in I$. Por lo tanto, existen $i,j \in I$ tales que $a'-a = i$ y $b'-b = j$. Entonces

$$a'b' = (a+i)(b+j) = ab+aj+ib+ij.$$

Dado que I es un ideal de R, se sigue que $aj, ib, ij \in I$. Por lo tanto, $a'b \in ab+I$. Es decir, $ab+I = a'b'+I$.

El resto de las propiedades que definen un anillo se verifican inmediatamente. Como ejemplo, verifiquemos una de las propiedades distributivas:

$$\begin{aligned}(a+I)((b+I)+(c+I)) &= (a+I)((b+c)+I)\\ &= a(b+c)+I\\ &= (ab+ac)+I\\ &= (ab+I)+(ac+I)\\ &= (a+I)(b+I)+(a+I)(c+I).\end{aligned}$$

El correspondiente elemento identidad en R/I es $1+I$. □

1.2.14 Ejemplo. En el anillo $\mathbb{Z}$ los ideales son de la forma $n\mathbb{Z}$ con $n>0$. En consecuencia, la estructura cociente $\mathbb{Z}/n\mathbb{Z}$ corresponde al conjunto $\mathbb{Z}_n$ de las clases de equivalencia de la relación congruencia módulo n. Esto es:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{k+n\mathbb{Z} \mid k = 0,1,\ldots,n-1\}.$$

1.3 Algunos tipos de anillos

Anillos de ideales principales

1.3.1 Definición. Sean R un anillo, $M \subseteq R$.

(1) El ideal `generado por` M, notado con (M) se define de la siguiente manera:

$$(M) := \bigcap \{I \mid I \text{ es un ideal de } R \text{ y } M \subseteq I\}.$$

(2) Si $M = \{m_1, \ldots, m_n\}$ es un conjunto finito, entonces (M) se dice `finitamente generado` y se escribe $(m_1, \ldots, m_n)$ en lugar de $(\{m_1, \ldots, m_n\})$.

(3) Si $M = \{m\}$, entonces (m) se denomina ideal `principal` de R. Si R es un dominio entero y todo ideal de R es principal, entonces R se llama un anillo de `ideales principales`.

1.3.2 Lema. Sean R un anillo con elemento identidad, M un subconjunto de R e I, J ideales de R.

(1) Si $M = \varnothing$, entonces $(M) = \{0\}$.

(2) (M) es el ideal más pequeño de R que contiene a M. Es decir, si I es un ideal de R y $M \subseteq I$, entonces se verifica que $(M) \subseteq I$.

(3) $(I \cup J) = I + J$. En particular, $I + J$ es el ideal más pequeño de R que contiene tanto a I como a J.

Demostración. Se deja como ejercicio. □

1.3.3 Lema. Sean R un anillo con elemento identidad, $\varnothing \neq M \subseteq R$ y $x \in R$. Entonces

(1) El ideal generado por x está dado por:

$$(x) = \Big\{ \sum_{i=1}^{m} r_i x s_i \mid r_i, s_i \in R,\ m \in \mathbb{N} \Big\}.$$

(2) Si $x \in \mathrm{Z}(R)$, entonces

$$(x) = xR = Rx = \{xr \mid r \in R\}.$$

(3) Si $M \subseteq \mathrm{Z}(R)$, entonces

$$(M) = \Big\{ \sum_{i=1}^{n} r_i m_i \mid r_i \in R,\ m_i \in M,\ n \in \mathbb{N} \Big\}.$$

(4) Si R es conmutativo, entonces

$$(M) = \Big\{ \sum_{i=1}^{n} r_i m_i \mid r_i \in R,\ m_i \in M,\ n \in \mathbb{N} \Big\}.$$

En particular, si $M = \{m_1, \ldots, m_k\}$, entonces

$$(m_1, \ldots, m_k) = m_1 R + \cdots + m_k R$$

y

$$(x) = xR = Rx = \{xr \mid r \in R\}.$$

Demostración. (1) Definamos el conjunto

$$I := \Big\{ \sum_{i=1}^{m} r_i x s_i \mid r_i, s_i \in R,\ m \in \mathbb{N} \Big\}.$$

Se verifica sin dificultades que I es un ideal de R y que $x \in I$. En consecuencia, $(x) \subseteq I$.

Sea J un ideal cualquiera de R con $x \in J$. Entonces $I \subseteq J$. De la definición de (x) se sigue que $I = (x)$.

(2) Se sigue de (1), ya que x conmuta con todo elemento de R.

(3) Demostremos inicialmente que el conjunto

$$I := \Big\{ \sum_{i=1}^{n} r_i m_i \mid r_i \in R,\ m_i \in M,\ n \in \mathbb{N} \Big\}$$

es un ideal de R. Si $m \in M$, entonces $m = 1m \in I$ y se sigue que $M \subseteq I$. En particular, $I \neq \varnothing$. Sean $x, y \in I$, digamos $x = \sum_{i=1}^{n} r_i m_i$ y $y = \sum_{i=1}^{k} r_i' m_i'$ con $r_i, r_i' \in R$ y $m_i, m_i' \in M$. Entonces

$$x - y = \sum_{i=1}^{n} r_i m_i - \sum_{i=1}^{k} r_i' m_i' \in I.$$

Esto demuestra que I es un subgrupo (aditivo) de R.

Si $r \in R$, entonces

$$rx = r \sum_{i=1}^{n} r_i m_i = \sum_{i=1}^{n} (r r_i) m_i \in I$$

y

$$xr = \sum_{i=1}^{n} r_i m_i r = \sum_{i=1}^{n} (r_i r) m_i \in I.$$

Sean ahora J un ideal de R con $M \subseteq J$, $m \in M$ y $r \in R$. Entonces $rm \in J$ y, por consiguiente, cualquier elemento de I pertenece a J. En resumen tenemos que $I = (M)$.

(4) Se sigue inmediatamente de (3). □

1.3.4 Ejemplos. (1) Todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{N}_0$. Por lo tanto, $\mathbb{Z}$ es un anillo de ideales principales.

(2) Si $m, n \in \mathbb{Z}$, $d := \text{mcd}(m, n)$ y $r := \text{mcm}(m, n)$, entonces

(a) $m\mathbb{Z} \cap n\mathbb{Z} = r\mathbb{Z}$

(b) $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$

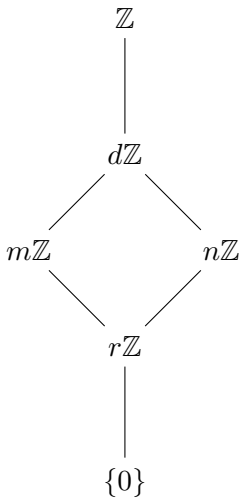
(3) Si $m, n \in \mathbb{Z}$, entonces $(m, n) = d\mathbb{Z}$. En efecto, del lema 1.3.3 se sigue que

$$(m, n) = \{rm + sn \mid r, s \in \mathbb{Z}\}. \tag{1.24}$$

Por otro lado, dados $m, n \in \mathbb{Z}$ siempre existen $a, b \in \mathbb{Z}$ tales que

$$d = \text{mcd}(m, n) = am + bn.$$

Por lo tanto, el conjunto del lado derecho en (1.24) no es más que el conjunto de los múltiplos de d. Es decir, $d\mathbb{Z}$.



Anillos noetherianos

1.3.5 Definición. Un anillo R se denomina `noetheriano` si se verifica que todo ideal I de R es finitamente generado. Es decir, existen $r_1, \ldots, r_m \in R$ tales que $I = (r_1, \ldots, r_m)$.

1.3.6 Ejemplos. (1) Todo cuerpo es un anillo noetheriano.

(2) Todo anillo de ideales principales es un anillo noetheriano. En particular $\mathbb{Z}$ lo es.

1.3.7 Teorema. Sea R un anillo cualquiera. Son equivalentes:

(1) R es un anillo noetheriano.

(2) Toda cadena ascendente de ideales propios de R

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k \subseteq \cdots \subseteq R$$

se estaciona. Es decir, existe $n \in \mathbb{N}$ tal que $I_n = I_{n+k}$ para todo $k \in \mathbb{N}$.

(3) Todo conjunto no vacío de ideales propios de R admite un elemento maximal.

Demostración. (1) $\Rightarrow$ (2). Sea $I := \bigcup_{k\in\mathbb{N}} I_k$. Dado que la cadena de ideales es ascendente, se verifica sin dificultades que I es un ideal propio de R. Por otro lado, dado que R es un anillo noetheriano se tiene que existen $r_1, \ldots, r_m \in R$ tales que $I = (r_1, \ldots, r_m)$. Por lo tanto, para cada r_j existe $n_j \in \mathbb{N}$ tales que $r_j \in I_{n_j}$. Si definimos

$$n := \max\{n_1, \ldots, n_m\},$$

entonces se verifica que $r_j \in I_n$ para todo j. Por lo tanto, $I \subseteq I_n$ y así $I = I_n$. En consecuencia, $I_n = I_{n+k}$ para todo $k \in \mathbb{N}$.

(2) $\Rightarrow$ (3). Si existiese un conjunto no vacío $\mathcal{M}$ de ideales propios de R que no contiene un elemento máximo, entonces para cualquier $I_1 \in \mathcal{M}$ existe $I_2 \in \mathcal{M}$ tal que $I_1 \subset I_2$. De esta manera se construye una cadena infinita ascendente de ideales propios de R que no se estaciona.

(3) $\Rightarrow$ (1). Sea I un ideal propio de R (los otros casos son triviales) y definamos

$$\mathcal{M} := \{A \mid (a_1, \ldots, a_m) = A \subseteq I\}.$$

Dado que $\{0\} \in \mathcal{M}$ se tiene que $\mathcal{M}$ es no vacío. Por hipótesis este conjunto tiene un elemento maximal, digamos $A = (a_1, \ldots, a_n) \subseteq I$. Supongamos que $A \subset I$. Entonces existe $a \in I \setminus A$ y se tendría que $A \subset (a_1, \ldots, a_m, a) \subseteq I$, lo cual contradice la maximalidad de A. □

1.3.8 Ejemplo. Sea $R = C^0(\mathbb{R})$ y para cada $n \in \mathbb{N}$ definamos $\Lambda_n := [0, \frac{1}{n}]$ y definamos además

$$I_n := \{f \in R \mid f|_{\Lambda_n} = 0\}.$$

Se verifica que cada I_n es un ideal de R y adicionalmente

$$I_1 \subset I_2 \subset \cdots.$$

Esto trae como consecuencia que R no es un anillo noetheriano.

1.3.9 Teorema. (Teorema de la base de Hilbert, 1888) Si R es un anillo conmutativo noetheriano, entonces $R[x]$ también lo es.

Demostración. Supongamos que $R[x]$ no es un anillo noetheriano y sea I un ideal de $R[x]$ que no es finitamente generado. Sea $f_1 \in I$ con grado mínimo $n_1 \geq 0$, digamos

$$f = a_1 x^{n_1} + \cdots$$

Dado que I no es finitamente generado, se tiene que $I \setminus (f_1) \neq \varnothing$. Elijamos en este conjunto un polinomio f_2 con grado mínimo $n_2 \geq 0$, digamos

$$f = a_2 x^{n_2} + \cdots$$

Supongamos que se han elegido $f_k \in I$ de tal forma que f_{k+1} sea un polinomio con grado mínimo perteneciente el conjunto

$$I \setminus (f_1, \ldots, f_k).$$

Para todo $k \in \mathbb{N}$, sean $n_k = \operatorname{grad}(f_k)$ y a_k el coeficiente principal de f_k. De la construcción anterior se sigue que

$$n_1 \leq n_2 \leq \ldots$$

y, además,

$$(a_1) \subseteq (a_1, a_2) \subseteq \ldots$$

Demostramos que estas inclusiones son propias. Es decir, la cadena de ideales no se estaciona. Para ello supongamos que para algún $k \in \mathbb{N}$ se verifica que

$$(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1}).$$

Entonces existirían $b_1, \ldots, b_k \in R$ tales que

$$a_{k+1} = \sum_{j=1}^{k} b_j a_j$$

y el polinomio

$$g := f_{k+1} - \sum_{j=1}^{k} b_j x^{n_{k+1} - n_j} f_j$$

pertenecería a $I \setminus (f_1, \ldots, f_k)$ y, además, tendría grado menor que f_{k+1}, lo cual no es posible. □

1.3.10 Corolario. Si R es un anillo conmutativo noetheriano, entonces $R[x_1, \ldots, x_n]$ también lo es.

DEMOSTRACIÓN. Usando inducción matemática sobre n y dado que $R[x_1,\ldots,x_n] = (R[x_1,\ldots,x_{n-1}])[x_n]$, se tiene la afirmación. □

1.3.11 Observación. D. Hilbert demostró el teorema de la base para $R = \mathbb{Z}$ y para todo cuerpo R.

1.3.12 Definición. Un ideal I de un anillo R se denomina `irreducible` si para todos J, T ideales de R se verifica:

$$I = J \cap T \Longrightarrow (I = J \vee I = T).$$

1.3.13 Ejemplo. Sean $R = \mathbb{Z}$ e $I = (p^n)$, donde p es un número primo y $n \in \mathbb{N}$. Si $(p^n) = (a) \cap (b) = (\text{mcm}(a,b))$, entonces se tiene que $a = \pm p^i$ y $b = p^j$, para algunos $i, j \in \{1,2,\ldots,n\}$. Esto trae como consecuencia que solo es posible que $\max\{i,j\} = n$. Por lo tanto, $I = (a)$ o $I = (b)$ y se tiene que I es un ideal irreducible.

1.3.14 Teorema. Todo ideal propio de un anillo noetheriano R es una intersección finita de ideales irreducibles.

DEMOSTRACIÓN. Procedemos por reducción al absurdo. Sea $\mathcal{I}$ el conjunto de todos los ideales J de R que no son intersección finita de ideales irreducibles de R y supongamos que $\mathcal{I}$ no es vacío. Por el teorema 1.3.7 se sigue que $\mathcal{I}$ tiene un elemento maximal, digamos M. Claramente M no es irreducible, ya que de lo contrario se contradice el hecho $M \in \mathcal{I}$. En consecuencia, $M = J \cap T$, para algunos ideales J, T de R tales que $J \neq M$ y $T \neq M$. Por otro lado, note que $M \subset J$ y $M \subset T$, así, por la maximalidad de M se tiene que $J \notin \mathcal{I}$ y $T \notin \mathcal{I}$. Entonces J y T son intersecciones finitas de ideales irreducibles y consecuentemente $M = J \cap T$ también lo sería, lo cual contradice $M \in \mathcal{I}$. En conclusión, nuestro supuesto inicial es falso, es decir, $\mathcal{I} = \varnothing$ con lo cual se tiene la demostración de la afirmación. □

Anillos euclidianos

1.3.15 Definición. Un dominio entero R se denomina `euclidiano` si existe una función $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ con la siguiente propiedad:

Para todo $a, b \in R \setminus \{0\}$ existen $q, r \in R$ tales que $a = bq + r$ con $r = 0$ o $r \neq 0$ y $\varphi(r) < \varphi(b)$.

1.3.16 Ejemplos. (1) $\mathbb{Z}$ es un anillo euclidiano. Como función φ puede considerarse el valor absoluto.

(2) Si K es un cuerpo, entonces el anillo $K[x]$ de los polinomios en una indeterminada es euclidiano. Esta afirmación se sigue del teorema de la división con resto. La función φ está dada por el grado.

(3) El anillo de los enteros gaussianos $\mathbb{Z}[\mathrm{i}]$ es euclidiano. Definamos φ de la siguiente manera:

$$\varphi(z) := z\bar{z}.$$

Es decir,

$$\varphi(x + y\mathrm{i}) := x^2 + y^2.$$

Sean $0 \neq a, b \in \mathbb{Z}[\mathrm{i}]$. Entonces $\frac{a}{b} = t + s\mathrm{i}$ con $t, s \in \mathbb{Q}$. Elijamos $m, n \in \mathbb{Z}$ tales que

$$|t - m| \leq \tfrac{1}{2} \quad \text{y} \quad |s - n| \leq \tfrac{1}{2}.$$

Es decir, m y n son los números enteros más cerca de t y s respectivamente. Definamos $q := m + n\mathrm{i}$. Entonces es claro que $q \in \mathbb{Z}[\mathrm{i}]$ y que $a = bq + r$ con $r := (a - bq)$.

Por otro lado, note que

$$\varphi(\tfrac{a}{b} - q) = \varphi(t + s\mathrm{i} - m - n\mathrm{i}) = (t - m)^2 + (s - n)^2 \leq \tfrac{1}{2}.$$

Por lo tanto, $r = 0$ o

$$\varphi(r) = \varphi(b(\tfrac{a}{b} - q)) = \varphi(b)\varphi(\tfrac{a}{b} - q) < \varphi(b).$$

(4) El anillo $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ es euclidiano. Definamos φ de la siguiente manera:

$$\varphi(x + y\mathrm{i}\sqrt{2}) := x^2 + 2y^2.$$

Sean $0 \neq a, b \in \mathbb{Z}[\mathrm{i}\sqrt{2}]$. Entonces $\frac{a}{b} = t + s\mathrm{i}\sqrt{2}$ con $t, s \in \mathbb{Q}$. Elijamos $m, n \in \mathbb{Z}$ tales que

$$|t - m| \leq \tfrac{1}{2} \quad \text{y} \quad |s - n| \leq \tfrac{1}{2}.$$

Nuevamente, m y n son los números enteros más cerca de t y s respectivamente. Definamos $q := m + n\mathrm{i}\sqrt{2}$. Entonces es claro que $q \in \mathbb{Z}[\mathrm{i}\sqrt{2}]$ y que $a = bq + r$ con $r := (a - bq)$.

Por otro lado, note que

$$\varphi(\tfrac{a}{b} - q) = \varphi(t + s\mathrm{i}\sqrt{2} - m - n\mathrm{i}\sqrt{2}) = (t - m)^2 + 2(s - n)^2 \leq \tfrac{3}{4}.$$

Por lo tanto, $r = 0$ o

$$\varphi(r) = \varphi(b(\tfrac{a}{b} - q)) = \varphi(b)\varphi(\tfrac{a}{b} - q) < \varphi(b).$$

1.3.17 Teorema. Si R es un anillo euclidiano, entonces R es un anillo de ideales principales.

DEMOSTRACIÓN. Sea R un anillo euclidiano y sea $I \neq \{0\}$ un ideal de R. Consideremos el conjunto

$$\mathcal{M} := \{\varphi(x) \mid 0 \neq x \in I\} \subseteq \mathbb{N}_0.$$

Dado que $I \neq \{0\}$ se tiene que $\mathcal{M} \neq \varnothing$. Usando el principio de buen orden se sigue que $\mathcal{M}$ tiene un elemento mínimo, digamos $\varphi(a)$ con $a \in I$.

Demostramos que $I = (a)$. Dado que R es euclidiano para todo $b \in I$ existen $q, r \in R$ tales que $a = bq + r$ con $r = 0$ o $r \neq 0$ y $\varphi(r) < \varphi(b)$. Note que $b \in I$, $aq \in I$, por consiguiente $r \in I$. Por la minimalidad de $\varphi(a)$ se sigue que $r = 0$ con lo cual se tiene que $I = (a)$. □

CAPÍTULO 2

HOMOMORFISMOS DE ANILLOS

2.1 Definiciones básicas, núcleo e imagen

2.1.1 Definición. Sean R y S anillos.

(1) Una función $\varphi : R \longrightarrow S$ se llama un `homomorfismo de anillos` si para todo $x, y \in R$ se verifican:

(a) $\varphi(x+y) = \varphi(x) + \varphi(y)$.
(b) $\varphi(xy) = \varphi(x)\varphi(y)$.

Notése que, en particular, φ es un homomorfismo entre los grupos $(R,+)$ y $(S,+)$. El conjunto de todos los homomorfismos de R en S lo notamos con $\mathrm{Hom}(R,S)$.

(2) Sea $\varphi \in \mathrm{Hom}(R,S)$. Si φ es biyectiva, entonces este se denomina un `isomorfismo`. En este caso escribimos $R \cong S$ y decimos que R y S son `isomorfos`. Esto podemos interpretarlo diciendo que R y S se diferencian solo en la forma de los elementos y que es posible identificar cada elemento de R con un único elemento de S. Si φ es inyectiva, entonces se dice que φ es un `monomorfismo`. Note que S contiene un subanillo isomorfo a $\varphi(R)$. En este caso es usual decir que R se puede sumergir en S y φ se llama una `inmersión` y R puede verse como un subanillo de S. Si φ es sobreyectiva, entonces se llama un `epimorfismo`.

(3) Si $\varphi \in \mathrm{Hom}(R,R)$, entonces decimos que φ es un `endomorfismo`. El conjunto de todos estos se nota con $\mathrm{End}(R)$. Un endomorfismo biyectivo de R se llama un `automorfismo` de R. El conjunto de estos se nota con $\mathrm{Aut}(R)$.

2.1.2 Ejemplos. (1) La función idénticamente nula define un homomorfismo estre dos anillos. Llamamos a esta el `homomorfismo nulo`.

(2) La función idéntica sobre un anillo R define un endomorfismo de R.

(3) La conjugación define un automorfismo de $\mathbb{C}$.

(4) Si R es un anillo con elemento identidad, entonces $\varphi : \mathbb{Z} \longrightarrow R$ definida por $\varphi(n) = n1$ para todo $n \in \mathbb{Z}$ es un homomorfismo de anillos.

(5) La función $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ definida por $\varphi(x) = [x]$ es un epimorfismo.

(6) La función $\varphi : \mathbb{C} \longrightarrow \mathrm{Mat}(2, \mathbb{R})$ definida por

$$\varphi(a + b\mathrm{i}) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

es un monomorfismo.

(7) Sean R un anillo, X un conjunto no vacío y $a \in X$ fijo. Entonces $\varphi_a : \mathrm{Fun}(X, R) \longrightarrow R$ definida por $\varphi_a(f) = f(a)$ es un endomorfismo de anillos.

(8) El grupo de automorfismos del grupo $(\mathbb{Z}, +)$ es isomorfo a $\mathbb{Z}_2$, sus elementos son $I(x) = x$ y $\varphi(x) = -x$ para todo $x \in \mathbb{Z}$. Dado que φ no es un homomorfismo de anillos, se sigue que el conjunto de los automorfismos de $\mathbb{Z}$ como anillo es $\{I\}$.

2.1.3 Lema. Sean R, S anillos, $\varphi \in \mathrm{Hom}(R, S)$, $x \in R$ y $n \in \mathbb{Z}$. Entonces

(1) $\varphi(0) = 0$.

(2) $\varphi(-x) = -\varphi(x)$.

(3) $\varphi(nx) = n\varphi(x)$.

Demostración. Se deja como ejercicio. □

2.1.4 Definición. Sean R, S anillos y $\varphi \in \mathrm{Hom}(R, S)$. Definimos y notamos respectivamente el `núcleo` y la `imagen` de φ de la siguiente manera:

(1) $\ker(\varphi) := \{r \in R \mid \varphi(r) = 0\}$.

(2) $\mathrm{Im}(\varphi) := \{\varphi(r) \mid r \in R\}$.

2.1.5 Ejemplos. (1) Sean R y S anillos. La función $\varphi : R \longrightarrow R \times S$ definida por

$$\varphi(x) := (x, 0)$$

es un homomorfismo. Note que $\varphi(1) \neq 1$. Los homomorfismos para los cuales se cumple que $\varphi(1) = 1$ se denominan `unitarios`. Se verifica además que

$$\ker(\varphi) = \{(0, 0)\}.$$

(2) Si I es un ideal de R, entonces la función $\pi : R \longrightarrow R/I$ definida por

$$\varphi(r) := r + I$$

es un epimorfismo, cuyo núcleo es I. Este se llama el `epimorfismo canónico`.

2.1.6 Lema. Sean R y S anillos y $\varphi \in \mathrm{Hom}(R, S)$. Entonces

(1) φ es un monomorfismo si y solo si $\ker(\varphi) = \{0\}$

(2) $\ker(\varphi)$ es un ideal de R

(3) $\mathrm{Im}(\varphi)$ es un subanillo de S

(4) Si S es un dominio entero y φ es un epimorfismo, entonces $\varphi(1) = 1$.

DEMOSTRACIÓN. (1) Se deja como ejercicio.

(2) Es claro que $(\ker(\varphi), +) \leq (R, +)$. Si $r \in R$ y $a \in \ker(\varphi)$, entonces

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(a)0 = 0.$$

Es decir, $ra \in \ker(\varphi)$. Similar se demuestra que $ar \in \ker(\varphi)$.

(3) Es claro que $(\mathrm{Im}(\varphi), +) \leq (S, +)$. Si $\varphi(a), \varphi(b) \in \mathrm{Im}(\varphi)$, entonces

$$\varphi(a)\varphi(b) = \varphi(ab) \in \mathrm{Im}(\varphi).$$

(4) Sea $0 \neq s \in S$. Entonces existe $r \in R$ tal que $s = \varphi(r)$. Entonces

$$\varphi(1)s = \varphi(1)\varphi(r) = \varphi(1r) = \varphi(r) = s.$$

Por lo tanto,

$$(\varphi(1) - 1)s = 0.$$

Dado que S es un dominio entero, se tiene que $\varphi(1) = 1$. □

2.1.7 Teorema. Sean R y S anillos, I un subanillo (ideal) de R, J un subanillo (ideal) de S y $\varphi \in \mathrm{Hom}(R,S)$. Entonces

(1) $\varphi(I)$ es un subanillo (ideal) de $\mathrm{Im}(\varphi)$

(2) $\varphi^{-1}(J)$ es subanillo (ideal) de R.

DEMOSTRACIÓN. Se deja como ejercicio. □

2.1.8 Teorema. (Correspondencia entre subanillos) Sea $\varphi \in \mathrm{Hom}(R,S)$. Notemos con $\mathscr{S}(R,\ker(\varphi))$ el conjunto de los subanillos de R que contienen a $\ker(\varphi)$ y con $\mathscr{S}(\mathrm{Im}(\varphi))$ el conjunto de los subanillos de $\mathrm{Im}(\varphi)$. Para $V \in \mathscr{S}(\mathrm{Im}(\varphi))$ sea $\varphi^{-1}(V) := \{x \in R \mid \varphi(x) \in V\}$. Entonces las funciones

$$\tau_1 : \mathscr{S}(R,\ker(\varphi)) \longrightarrow \mathscr{S}(\mathrm{Im}(\varphi))$$

definida por

$$\tau_1(U) = \varphi(U)$$

y

$$\tau_2 : \mathscr{S}(\mathrm{Im}(\varphi)) \longrightarrow \mathscr{S}(R,\ker(\varphi))$$

definida por

$$\tau_2(V) = \varphi^{-1}(V)$$

son biyectivas y una es la inversa de la otra.

DEMOSTRACIÓN. Sea $U \in \mathscr{S}(R,\ker(\varphi))$. Es claro por el teorema anterior que $\tau_1(U) \in \mathscr{S}(\mathrm{Im}(\varphi))$.

(1) Demostramos que τ_1 es inyectiva. Sean $U, U' \in \mathscr{S}(R,\ker(\varphi))$ para los cuales se verifica que $\tau_1(U) = \tau_1(U')$. Es decir, $\varphi(U) = \varphi(U')$.

Sea $x \in U$. Entonces existe $y \in U'$ tal que $\varphi(x) = \varphi(y)$. En consecuencia, $x - y \in \ker(\varphi) \subseteq U'$. Por lo tanto, $x - y \in U'$ y se sigue que $x \in U'$. Esto es, $U \subseteq U'$. Similar se demuestra que $U' \subseteq U$, concluyendo que $U = U'$.

(2) Demostramos que τ_1 es sobreyectiva. Sea $V \in \mathscr{S}(\mathrm{Im}(\varphi))$ y definamos $U := \varphi^{-1}(V)$. Del teorema anterior se sigue que U es un subanillo de R. Si $u \in \ker(\varphi)$, entonces $\varphi(u) = 0 \in V$ con lo cual se tiene que $u \in U$. Esto demuestra que $\ker(\varphi) \subseteq U$. Es decir, $U \in \mathscr{S}(R,\ker(\varphi))$. Finalmente, note que

$$V = \varphi(\varphi^{-1}(V)) = \varphi(U) = \tau_1(U).$$

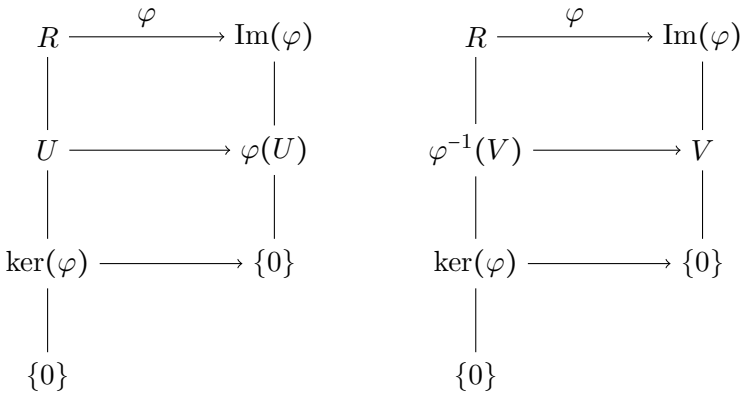
(3) Se deja como ejercicio demostrar que τ_2 es una función biyectiva.

(4) Para probar la última afirmación, sea $V \in S(\mathrm{Im}(\varphi))$. Entonces

$$\tau_1(\tau_2(V)) = \tau_1(\varphi^{-1}(V)) = \varphi(\varphi^{-1}(V)) = V.$$

Es decir, $\tau_1 \circ \tau_2 = I_{\mathscr{S}(\mathrm{Im}(\varphi))}$.

El siguiente gráfico ilustra el teorema.



2.1.9 Teorema. (Correspondencia entre ideales) Sea $\varphi \in \mathrm{Hom}(R, S)$. Notemos con $\mathscr{I}(R, \ker(\varphi))$ el conjunto de los ideales de R que contienen a $\ker(\varphi)$ y con $\mathscr{I}(\mathrm{Im}(\varphi))$ el conjunto de los ideales de $\mathrm{Im}(\varphi)$. Las funciones

$$\tau_1 : \mathscr{I}(R, \ker(\varphi)) \longrightarrow \mathscr{I}(\mathrm{Im}(\varphi))$$

definida por

$$\tau_1(I) = \varphi(I)$$

y

$$\tau_2 : \mathscr{I}(\mathrm{Im}(\varphi)) \longrightarrow \mathscr{I}(R, \ker(\varphi))$$

definida por

$$\tau_2(V) = \varphi^{-1}(V)$$

son biyectivas y una es la inversa de la otra.

Demostración. Similar como en el teorema anterior. □

2.2 Teoremas de isomorfía

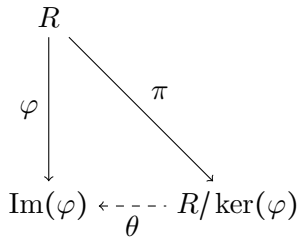
2.2.1 Teorema. (Isomorfía I) Sean R y S anillos y $\varphi \in \mathrm{Hom}(R,S)$. Entonces la función $\theta : R/\ker(\varphi) \longrightarrow \mathrm{Im}(\varphi)$ definida por

$$\theta(r+\ker(\varphi)) = \varphi(r), \qquad r \in R$$

es un isomorfismo. Es decir,

$$R/\ker(\varphi) \cong \mathrm{Im}(\varphi) \tag{2.1}$$

Ilustración:



Demostración. Sea π el epimorfismo canónico de R en $R/\ker(\varphi)$.

(1) θ `está bien definida.` Sean $x, y \in R$.

$$\begin{aligned} x+\ker(\varphi) = y+\ker(\varphi) &\Leftrightarrow x-y \in \ker(\varphi) \\ &\Leftrightarrow \varphi(x-y) = 0 \\ &\Leftrightarrow \varphi(x)-\varphi(y) = 0 \\ &\Leftrightarrow \varphi(x) = \varphi(y) \\ &\Leftrightarrow \theta(x+\ker(\varphi)) = \theta(y+\ker(\varphi)). \end{aligned}$$

(2) θ `es un homomorfismo.` Sean $x, y \in R$.

$$\begin{aligned} \theta((x+\ker(\varphi))+(y+\ker(\varphi))) &= \theta((x+y)+\ker(\varphi)) \\ &= \varphi(x+y) \\ &= \varphi(x)+\varphi(y) \\ &= \theta(x+\ker(\varphi))+\theta(y+\ker(\varphi)). \end{aligned}$$

Por otro lado,

$$\begin{aligned} \theta((x+\ker(\varphi))\cdot(y+\ker(\varphi))) &= \theta(xy+\ker(\varphi)) \\ &= \varphi(xy) \\ &= \varphi(x)\varphi(y) \\ &= \theta(x+\ker(\varphi))\cdot\theta(y+\ker(\varphi)). \end{aligned}$$

(3) θ `es un epimorfismo.` Evidente.

(4) Finalmente,

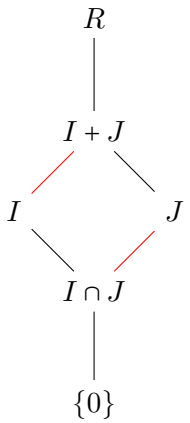
$$\begin{aligned}\ker(\theta) &= \{x + \ker(\varphi) \mid \varphi(x) = 0\} \\ &= \{x + \ker(\varphi) \mid x \in \ker(\varphi)\} \\ &= \{\ker(\varphi)\}.\end{aligned}$$

En resumen se tiene que $R/\ker(\varphi) \cong \mathrm{Im}(\varphi)$. □

2.2.2 Teorema. (Isomorfía II) Sean R un anillo, I un ideal de R y J un subanillo de R. Entonces

$$J/(I \cap J) \cong (I + J)/I.$$

Ilustración:



Demostración. Se verifica sin dificultades que $I \cap J$ es un ideal de J y claramente I es un ideal de $I + J$. Sea

$$\varphi : J \longrightarrow (I + J)/I$$

definida por

$$\varphi(j) = j + I.$$

(1) φ `está bien definida.` Sean $x, y \in J$. Si $x = y$, entonces $x - y = 0 \in I$. Por consiguiente, $(x - y) + I = I$ y se tiene que $x + I = y + I$.

(2) φ `es un homomorfismo de anillos.` Sean $x, y \in I$. Entonces

$$\varphi(x + y) = (x + y) + I = (x + I) + (y + I) = \varphi(x) + \varphi(y).$$

Por otro lado,

$$\varphi(xy) = xy + I = (x + I) \cdot (y + I) = \varphi(x)\varphi(y).$$

(3) φ `es sobre.` Sea $x + I \in (I + J)/I$. Entonces $x = i + j$ con $i \in I$ y $j \in J$. Por lo tanto,

$$x + I = (i + j) + I = j + I = \varphi(j).$$

(4) Finalmente,

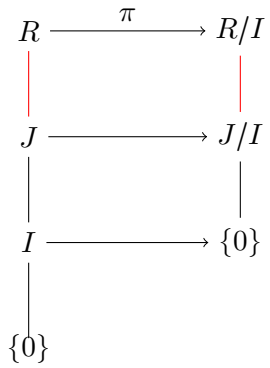
$$\ker(\varphi) = \{j \in J \mid j + I = I\} = \{j \in J \mid j \in I\} = I \cap J.$$

La conclusión se sigue del primer teorema de isomorfía. □

2.2.3 Teorema. (Isomorfía III) Sean R un anillo e I, J ideales de R con $I \subseteq J$. Entonces

$$(R/I)/(J/I) \cong R/J.$$

Ilustración:



Demostración. Demostramos inicialmente que J/I es un ideal de R/I. Dado que J es un ideal de R, tiene sentido el cociente J/I a través del epimorfismo canónico π. Naturalmente J/I es un subgrupo aditivo de R/I. Sean ahora $r + I \in R/I$ y $k + I \in J/I$. Entonces

$$(r + I)(k + I) = rk + I \in J/I.$$

Consideremos ahora la función $\varphi : R/I \longrightarrow R/J$ definida por

$$\varphi(x + I) = x + J, \qquad x \in R.$$

(1) φ `está bien definida.` Sean $x, y \in R$.

$$\begin{aligned} x + I = y + I &\Leftrightarrow x - y \in I \\ &\Leftrightarrow x - y \in J \\ &\Leftrightarrow x + J = y + J \\ &\Leftrightarrow \varphi(x + I) = \varphi(y + I). \end{aligned}$$

(2) φ `es un homomorfismo de anillos.` Sean $x, y \in R$.

$$\begin{aligned}\varphi((x+I)+(y+I)) &= \varphi((x+y)+I)\\ &= (x+y)+J\\ &= (x+J)+(y+J)\\ &= \varphi(x+I)+\varphi(y+I).\end{aligned}$$

Similar se demuestra que $\varphi((x+I)\cdot(y+I)) = \varphi(x+I)\varphi(y+I)$.

(3) Note que

$$\ker(\varphi) = \{x+I \mid x \in J\} = J/I.$$

(4) θ `es un epimorfismo.` Evidente.

La conclusión se sigue del primer teorema de isomorfía. □

2.2.4 Observación. Demostramos a continuación que todo anillo R sin elemento identidad puede sumergirse en otro anillo R^* que si tiene uno.

Sea R un anillo sin elemento identidad y consideremos $R^* := \mathbb{Z} \times R$ y definamos sobre R^* una adición y multiplicación de la siguiente manera:

$$\begin{aligned}(n_1, r_1) + (n_2, r_2) &= (n_1 + n_2, r_1 + r_2),\\ (n_1, r_1) \cdot (n_2, r_2) &= (n_1 n_2, n_1 r_2 + n_2 r_1 + r_1 r_2).\end{aligned}$$

Se verifica sin dificultades que R^* es un anillo y $(1, 0)$ es su elemento identidad.

Consideremos ahora la función $\iota : R \longrightarrow R^*$ definida por

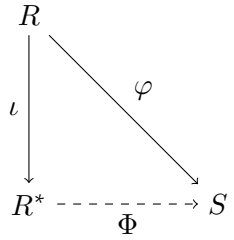
$$\iota(r) = (0, r).$$

Se demuestra fácilmente que ι es un homomorfismo de anillos y además

$$\ker(\iota) = \{r \in R \mid (0, r) = (0, 0)\} = \{0\}.$$

Es decir, ι es inyectiva.

Esta función ι satisface además la siguiente propiedad universal: dados un anillo S con elemento identidad y un homomorfismo de anillos $\varphi : R \longrightarrow S$, existe un único homomorfismo de anillos $\Phi : R^* \longrightarrow S$ tal que $\varphi = \Phi \circ \iota$.



La función Φ puede ser definida por $\Phi(n,r) = n1 + \varphi(r)$. En conclusión, se tiene que R^* es el anillo más general con elemento identidad que contiene a R.

Consideremos la función $\pi : R^* \longrightarrow \mathbb{Z}$ definida por $\pi(n,r) = n$. Se verifica que π es un epimorfismo de anillos y, además,

$$\ker(\pi) = \{(0,r) \in R^* \mid r \in R\} = \mathrm{Im}(\iota) \cong R.$$

En consecuencia, R puede verse como un ideal de R^* y, además, el anillo cociente R^*/R es isomorfo a $\mathbb{Z}$. En resumen, todo anillo sin elemento identidad es ideal de algún anillo.

2.3 El cuerpo cociente de un dominio entero

En el siguiente teorema demostramos que dado un dominio entero R, siempre existe un cuerpo $Q(R)$, en el cual puede sumergirse R como subanillo. En particular, el siguiente teorema nos permite construir el cuerpo $\mathbb{Q}$ a partir de $\mathbb{Z}$.

2.3.1 Lema. Sean R un dominio entero y $M := R \times R^\times$. Esto es,

$$M = \{(a,b) \mid a,b \in R,\ b \neq 0\}.$$

Si definimos sobre M la siguiente relación $\sim$

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc,$$

entonces $\sim$ es una relación de equivalencia.

Demostración. (1) Dado que $ab = ba$, se tiene que $(a,b) \sim (a,b)$.

(2) Supongamos que $(a,b) \sim (c,d)$. Entonces $ad = bc$, lo cual es equivalente a $cb = da$. Es decir, $(c,d) \sim (a,b)$.

(3) Supongamos que $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$.

$$\begin{aligned}
(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) &\Rightarrow ad = bc \ \wedge \ cf = de \\
&\Rightarrow adf = bde \\
&\Rightarrow d(af - be) = 0 \\
&\Rightarrow af = be \\
&\Rightarrow (a,b) \sim (e,f).
\end{aligned}$$

La clase de equivalencia de $(a,b) \in M$ se nota con $\frac{a}{b}$ en lugar de la notación usual $[(a,b)]$. Entonces

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

2.3.2 Lema. Sean R un dominio entero y $Q(R)$ el conjunto

$$Q(R) := \left\{ \frac{a}{b} \mid a, b \in R,\ b \neq 0 \right\}.$$

Si definimos sobre $Q(R)$ las siguientes operaciones:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \tag{2.2}$$

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}, \tag{2.3}$$

entonces $(Q(R), +, \cdot)$ es un cuerpo, el cual se denomina `cuerpo cociente` de R o `cuerpo de fracciones` de R.

Demostración. Es necesario verificar que estas operaciones están bien definidas. Es decir, que no dependen de los representantes que se tomen en las clases de equivalencias. Supongamos entonces que

$$\frac{a}{b} = \frac{e}{f} \quad \text{y} \quad \frac{c}{d} = \frac{g}{h}.$$

Entonces

$$af = eb \quad \text{y} \quad ch = gd. \tag{2.4}$$

En consecuencia, $acfh = bdeg$ y se tiene que

$$\frac{ac}{bd} = \frac{eg}{fh}.$$

Es decir,

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{e}{f} \cdot \frac{g}{h}.$$

Con lo cual se demuestra que la multiplicación está bien definida.

Por otro lado, de (2.4) se sigue que

$$\begin{aligned} bd(eh + fg) &= bdeh + bdfg \\ &= adfh + bcfh \\ &= fh(ad + bc). \end{aligned}$$

Por lo tanto,

$$\frac{ad + bc}{bd} = \frac{eh + fg}{fh}.$$

Es decir,

$$\frac{a}{b} + \frac{c}{d} = \frac{e}{f} + \frac{g}{h}.$$

Con lo cual se tiene que la suma está bien definida.

Se demuestra sin dificultades que $(Q(R), +, \cdot)$ es un cuerpo. El elemento neutro para la suma es $0 = \frac{0}{1}$, mientras que el elemento identidad es $1 = \frac{1}{1}$. Se verifica además que

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b} \quad \text{y} \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

(1) Inmersión de R en $Q(R)$. El dominio entero R puede verse como un subanillo del cuerpo $Q(R)$. En efecto, sea $\iota : R \longrightarrow Q(R)$ definida por

$$\iota(r) = \frac{r}{1}.$$

Entonces

(a) ι es un homomorfismo. Sea $r, s \in R$. Entonces

$$\iota(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = \iota(r) + \iota(s).$$

y

$$\iota(rs) = \frac{rs}{1} = \frac{r}{1}\frac{s}{1} = \iota(r)\iota(s).$$

(b) ι es inyectiva. Si $\iota(r) = \iota(s)$, entonces $\frac{r}{1} = \frac{s}{1}$ con lo cual se obtiene $r = s$.

(2) La propiedad universal. Esta establece que dado un monomorfismo φ

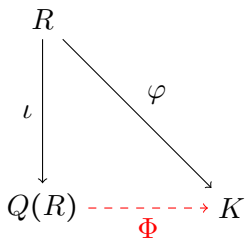
$$\varphi : R \longrightarrow K$$

y una vez sumergido R en $Q(R)$ mediante la función ι, existe una única forma de extender a ι mediante un monomorfismo de $Q(R)$ hasta el cuerpo K.

2.3.3 Teorema. (La propiedad universal) Sean ι la inmersión del dominio entero R en $Q(R)$ y K un cuerpo. Entonces para todo monomorfismo $\varphi : R \longrightarrow K$ existe un único monomorfismo $\Phi : Q(R) \longrightarrow K$ tal que

$$\varphi = \Phi \circ \iota. \tag{2.5}$$

Es decir, el siguiente diagrama conmuta.



Demostración. Demostramos que existe a lo más un monomorfismo $\Phi : Q(R) \longrightarrow K$ con la propiedad (2.5). Si $a, b \in R$ con $b \neq 0$, entonces debe cumplirse que

$$\begin{aligned}\Phi(\tfrac{a}{b}) &= \Phi\big(\tfrac{a}{1} \cdot \tfrac{1}{b}\big) \\ &= \Phi(\iota(a)\iota(b)^{-1}) \\ &= \Phi(\iota(a))\Phi(\iota(b)^{-1}) \\ &= \varphi(a)\varphi(b)^{-1}.\end{aligned}$$

Es decir, todo monomorfismo que satisface (2.5) es de la forma

$$\Phi(\tfrac{a}{b}) := \varphi(a)\varphi(b)^{-1}, \tag{2.6}$$

para todo $\frac{a}{b} \in Q(R)$.

(1) Φ `está bien definida.` Si $\frac{a}{b} = \frac{a'}{b'}$, entonces $ab' = a'b$ y se tiene que

$$\varphi(a)\varphi(b') = \varphi(ab') = \varphi(a'b) = \varphi(a')\varphi(b).$$

Por lo tanto,

$$\Phi(\tfrac{a}{b}) = \varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1} = \Phi(\tfrac{a'}{b'}).$$

(2) Φ `es homomorfismo.` Sean $\frac{a}{b}, \frac{c}{d} \in Q(R)$. Entonces

$$\begin{aligned}\Phi(\tfrac{a}{b} + \tfrac{c}{d}) &= \Phi(\tfrac{ad+bc}{bd}) \\ &= \varphi(ad + bc)\varphi(bd)^{-1} \\ &= (\varphi(a)\varphi(d) + \varphi(b)\varphi(c))\varphi(b)^{-1}\varphi(d)^{-1} \\ &= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} \\ &= \Phi(\tfrac{a}{b}) + \Phi(\tfrac{c}{d}).\end{aligned}$$

Similar se demuestra que

$$\Phi(\tfrac{a}{b} \cdot \tfrac{c}{d}) = \Phi(\tfrac{a}{b})\Phi(\tfrac{c}{d}).$$

(3) Φ `es inyectiva.` Sean $a, b \in R$ con $b \neq 0$ y supongamos que $\Phi(\frac{a}{b}) = 0$. Entonces $\varphi(a)\varphi(b)^{-1} = 0$. Dado que φ es inyectiva, se sigue que $a = 0$. Por lo tanto, $\frac{a}{b} = 0$. □

2.3.4 Ejemplos. Cuerpos cocientes.

(1) El cuerpo cociente de $\mathbb{Z}$ es isomorfo a $\mathbb{Q}$.

(2) El cuerpo cociente de $\mathbb{Z}[\mathrm{i}]$ es $\mathbb{Q}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Q}\}$.

(3) Si ζ es una raíz cúbica compleja de la unidad, entonces el cuerpo cociente de $\mathbb{Z}[\zeta]$ es $\mathbb{Q}[\zeta]$.

2.4 Ejercicios

(1) Sea R un dominio entero. Demuestre que las siguientes afirmaciones son equivalentes:

- (a) R es un cuerpo.
- (b) $R[x]$ es un anillo euclidiano.
- (c) $R[x]$ es un anillo de ideales principales.

(2) Sean R y S anillos y $\varphi \in \mathrm{Hom}(R, S)$. Entonces

- (a) Si $\varphi(1) \in U(S)$, entonces $\varphi(1) = 1$.
- (b) Si $0 \neq r \in R$ y $\varphi(r)$ no es un divisor de cero, entonces $\varphi(1) = 1$.
- (c) Si $\varphi(U(R)) \subseteq U(S)$, entonces $\varphi(1) = 1$.

(3) Sean R y S anillos y $\varphi \in \mathrm{Hom}(R, S)$ sobreyectiva. Si $\{U_j \mid j \in J\}$ es un conjunto de subanillos de R que contienen a $\ker(\varphi)$, demuestre que

$$\varphi\left(\bigcap_{j\in J} U_j\right) = \bigcap_{j\in J} \varphi(U_j).$$

CAPÍTULO 3

OTRAS PROPIEDADES DE LOS IDEALES

3.1 Ideales maximales e ideales primos

En esta sección consideramos dos clases especiales de ideales de un anillo R, los maximales y los primos. Los resultados centrales podemos resumirlos así: todo anillo admite un ideal maximal, si R es un anillo conmutativo y J es un ideal de R, entonces R/J es un dominio entero si y solo si J es un ideal primo y R/J es un cuerpo si y solo si J es un ideal maximal. Finalmente presentamos una relación entre estos tipos de ideales. Concretamente demostramos que todo ideal maximal en un anillo conmutativo es un ideal primo.

3.1.1 Definición. Sean R un anillo y $M \neq R$ un ideal. Decimos que M es un ideal `maximal` si se verifica alguna de las dos siguientes condiciones:

(1) Si I es un ideal de R y $M \subseteq I \subset R$, entonces $I = M$.

(2) Si I es un ideal de R y $M \subset I \subseteq R$, entonces $I = R$.

3.1.2 Ejemplos. (1) Si R es un cuerpo, entonces $\{0\}$ es un ideal maximal.

(2) Sea $n \in \mathbb{Z}$. Si $n = ab$ con $a, b \neq \pm 1$, entonces se verifica que $n\mathbb{Z} \subseteq a\mathbb{Z}$. Esto trae como consecuencia que los ideales maximales de $\mathbb{Z}$ son de la forma $p\mathbb{Z}$, donde p es un número primo.

(3) Si p es un número primo, entonces $I = (x, p)$ es un ideal maximal en $\mathbb{Z}[x]$.

3.1.3 Teorema. Sean R un anillo y M un ideal de R. Entonces,

(1) M es maximal si y solo si R/M es simple.

(2) Si en particular R es un anillo conmutativo con elemento identidad, entonces M es maximal si y solo si R/M es un cuerpo.

Demostración.

(1) Considerando el homomorfismo canónico $\pi : R \longrightarrow R/M$ y el teorema de correspondencia se tiene la afirmación.

(2) Se sigue del teorema 1.2.6. □

El siguiente teorema demostrado por W. Krull[1] afirma que en un anillo R siempre existen ideales maximales. Para demostrarlo hacemos uso del lema de Zorn[2], el cual presentamos a continuación.

3.1.4 Lema. (M. Zorn) Sea M un conjunto no vacío, parcialmente ordenado. Si toda cadena de M tiene una cota superior en M, entonces existe por lo menos un elemento maximal en M.

3.1.5 Teorema. (W. Krull) Sea R un anillo e $I \neq R$ un ideal de R. Entonces existe un ideal maximal M en R con $I \subseteq M$.

Demostración. Definamos el conjunto $\mathcal{M}$ mediante

$$\mathcal{M} := \{J \mid J \text{ es ideal de } R \text{ y } I \subseteq J \subset R\}.$$

Note que $I \in \mathcal{M}$, por lo tanto, $\mathcal{M}$ es no vacío y con respecto a la inclusión $\mathcal{M}$ es parcialmente ordenado.

Sea $\mathcal{C} \neq \varnothing$ una cadena de $\mathcal{M}$. Es decir, si $X, Y \in \mathcal{C}$, entonces $X \subseteq Y$ o $Y \subseteq X$.

Si definimos

$$J := \bigcup\{X \mid X \in \mathcal{C}\},$$

entonces J es un ideal de R, $I \subseteq J$ y $J \neq R$. Por lo tanto, $J \in \mathcal{M}$ y J es una cota superior para $\mathcal{C}$. Del lema de Zorn se sigue que $\mathcal{M}$ tiene un elemento maximal en $\mathcal{M}$. □

3.1.6 Corolario. Todo anillo R admite ideales maximales.

[1] Wolfgang Krull (Baden-Baden, 1899 - Bonn, 1971) fue un matemático alemán, especialista en álgebra conmutativa.

[2] Max August Zorn (Krefeld, 1906 - Bloomington, 1993) matemático alemán nacionalizado estadounidense.

DEMOSTRACIÓN. Es suficiente tomar en el teorema anterior $I = \{0\}$. □

3.1.7 Corolario. Sean R un anillo conmutativo con elemento identidad y $\{M_i \mid i \in I\}$ el conjunto de los ideales maximales de R. Entonces todo $x \in R \setminus \bigcup_{i\in I} M_i$ es invertible.

DEMOSTRACIÓN. Sea $x \in R \setminus \bigcup_{i\in I} M_i$. La conmutatividad de R garantiza que $(x) = xR$. Si $(x) \neq R$, entonces usando el teorema de Krull se tiene que $x \in (x) \subseteq M_i$ para algún $i \in I$, lo cual no es posible. En consecuencia, $(x) = xR = R$ y existe $y \in R$ tal que $xy = 1$. □

3.1.8 Teorema. Sea R un anillo y $P \neq R$ un ideal. Las siguientes afirmaciones son equivalentes:

(1) Para todo I, J ideales de R se verifica:

$$(P \subset I \wedge P \subset J) \Rightarrow IJ \nsubseteq P$$

(2) Para todo I, J ideales de R se verifica:

$$IJ \subseteq P \Rightarrow (I \subseteq P \vee J \subseteq P)$$

(3) Para todo $a, b \in R$ se verifica:

$$aRb \subseteq P \Rightarrow (a \in P \vee b \in P)$$

(4) Para todo $a, b \in R$ se verifica:

$$(a)(b) \subseteq P \Rightarrow (a \in P \vee b \in P)$$

DEMOSTRACIÓN. (1) ⇒ (2). Supongamos que se cumple (1) y supongamos además que existen ideales I, J de R tales que $IJ \subseteq P$ y $I \nsubseteq P$ y $J \nsubseteq P$. Entonces se tendría que $P \subset I + P$ y $P \subset J + P$ y también que

$$(I + P)(J + P) = IJ + IP + PJ + PP \subseteq IJ + P \subseteq P,$$

lo cual contradice nuestra hipótesis (1).

(2) ⇒ (3). Supongamos que $aRb \subseteq P$ para todo $a, b \in R$. Entonces $(RaR)(RbR) \subseteq P$. Si para $a \in R$, definamos $RaR := R(aR) = (Ra)R$, entonces se verifica que RaR es un ideal de R. Por lo tanto, $RaR \subseteq P$ o $RbR \subseteq P$.

`Caso 1.` Si $RaR \subseteq P$, entonces de $(a)(a)(a) \subseteq R(a)R = RaR \subseteq P$, usando (2) se sigue que $(a) \subseteq P$ y, en consecuencia, $a \in P$.

`Caso 2.` Si $RbR \subseteq P$, entonces de manera similar se demuestra que $b \in P$.

(3) $\Rightarrow$ (4). Supongamos que $(a)(b) \subseteq P$. Usando (3), dado que $aRb \subseteq (a)(b) \subseteq P$ se sigue que $a \in P$ o $b \in P$.

(4) $\Rightarrow$ (1). Sean I, J ideales de R y supongamos que $IJ \subseteq P$ y que, $I \nsubseteq P$. Entonces existe $a \in I \setminus P$. Para este a y para $b \in J$ cualquiera, se verifica que $(a)(b) \subseteq P$ y $(a) \nsubseteq P$. Usando (4) se sigue que $b \in P$. Dado que $b \in J$ fue arbitrario, se sigue que $J \subseteq P$. □

3.1.9 Definición. Sea R un anillo y $P \neq R$ un ideal. Decimos que P es un `ideal primo` de R si satisface alguna (por lo tanto todas) de las condiciones del teorema anterior. Si en particular $\{0\}$ es un ideal primo de R, entonces se dice que R es un `anillo primo`.

3.1.10 Corolario. Sea R un anillo conmutativo y $P \neq R$ un ideal. Entonces P es un ideal primo si y solo si para todo $a, b \in R$ se verifica:

$$ab \in P \Rightarrow (a \in P \vee b \in P).$$

En particular, R es un anillo primo si y solo si R no tiene divisores de cero.

Demostración. Dado que R es conmutativo, se sigue que $(ab) = (a)(b)$. El resto es aplicar el teorema anterior. □

3.1.11 Teorema. Sea R un anillo conmutativo con elemento identidad y P un ideal de R. Entonces P es un ideal primo si y solo si R/P es un dominio entero.

Demostración. Supongamos que P es un ideal primo y que

$$(a + P)(b + P) = P.$$

Entonces $ab \in P$ y se verifica que $a \in P$ o $b \in P$. Es decir, $a + P = P$ o $b + P = P$, lo cual demuestra que R/P no tiene divisores de cero.

Recíprocamente, supongamos que R/P es un dominio entero y sean A, B ideales de R con $AB \subseteq P$. Supongamos además que $A \nsubseteq P$ y $B \nsubseteq P$. Entonces existen $a \in A \setminus P$ y $b \in B \setminus P$ tales que $a + P \neq P$ y $b + P \neq P$. En consecuencia, $ab \in AB \subseteq P$. Por lo tanto,

$$(a + P)(b + P) = ab + P = P,$$

lo cual no es posible ya que R/P es un dominio entero. □

3.1.12 Ejemplos. (1) Sea $n \in \mathbb{N}$. Entonces $n\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ si y solo si n es un número primo.

(2) Si R es un dominio entero, entonces $\{0\}$ es un ideal primo.

(3) Si R es un dominio entero, entonces (x) es un ideal primo de $R[x]$.

3.1.13 Teorema. Todo ideal maximal de un anillo conmutativo R es un ideal primo.

DEMOSTRACIÓN. Si M es un ideal maximal de R, entonces del teorema 3.1.3 se sigue que R/M es un cuerpo y, en particular, un dominio entero. La conclusión se sigue del teorema anterior. □

3.1.14 Observación. En general, el recíproco del teorema anterior es falso. Por ejemplo, $\{0\}$ es un ideal primo de $\mathbb{Z}$, pero $\{0\}$ no es un ideal maximal.

3.1.15 Teorema. Sea R un anillo y $P \neq R$ un ideal primo de R. Entonces P es irreducible.

DEMOSTRACIÓN. Sea $P \neq R$ un ideal primo de R y supongamos que $P = J \cap T$. Entonces $JT \subseteq J \cap T = P$. Dado que P es un ideal primo, del teorema 3.1.8 se sigue que $J \subseteq P$ o $T \subseteq P$. Si se verifica que $J \subseteq P$, entonces $J \subseteq P = J \cap T \subseteq T$. Por lo tanto, $P = J \cap T = J$. De manera similar se demuestra que, si $T \subseteq P$, entonces $P = T$. □

3.1.16 Observación. El ejemplo 1.3.13 demuestra que el recíproco del teorema anterior es, en general, falso. En efecto, para $n > 1$ el ideal (p^n) no es primo.

3.2 Nilpotencia

3.2.1 Definición. Un ideal I de un anillo R se denomina `nilpotente` si existe $n \in \mathbb{N}$ tal que $I^n = \{0\}$. El número más pequeño n con tal propiedad se llama `grado de nilpotencia` de I. Similar se define esta propiedad para ideales izquierdos o derechos.

3.2.2 Ejemplo. Sea $R = \mathrm{T}(n, K)$ el anillo de las matrices triangulares superiores de tamaño $n \times n$ con entradas en un cuerpo K. Sea I el subconjunto de R formado por las matrices estrictamente superiores, es decir, matrices triangulares con ceros en la diagonal principal. Entonces I es un ideal de R que satisface $I^n = \{0\}$ y $I^{n-1} \neq \{0\}$.

3.2.3 Lema. Toda suma finita de ideales izquierdos (derechos) nilpotentes de un anillo R es un ideal izquierdo (derecho) nilpotente.

DEMOSTRACIÓN. Procedemos por inducción sobre el número k de sumandos.

Caso $k = 2$. Sean I, J ideales izquierdos nilpotentes de R. Entonces existen $n, m \in \mathbb{N}$ tales que $I^n = \{0\} = J^m$. Demostramos ahora que $(I + J)^{m+n-1} = \{0\}$. Usando el lema 1.2.12 (4), se tiene que $(I + J)^{m+n-1}$ puede expresarse como una suma de productos de

potencias de I y de J y en cada sumando aparece I^j con $j \geq n$ o aparece J^k con $k \geq m$. Por lo tanto, $(I+J)^{m+n-1} = \{0\}$.

El resto de la prueba es inmediato. □

3.2.4 Lema. Todo ideal izquierdo (derecho) nilpotente de un anillo R está contenido en un ideal nilpotente.

Demostración. Sea I un ideal izquierdo nilpotente de R. Es claro que IR es también un ideal nilpotente. Usando el lema anterior se sigue que $I + IR$ es nilpotente y además se cumple que $I \subseteq I + IR$. Similar se demuestra la afirmación si I es un ideal derecho. □

3.2.5 Definición. Sea R un anillo. Un elemento $x \in R$ se denomina `nilpotente` si existe $n \in \mathbb{N}$ tal que $x^n = 0$. Un ideal izquierdo (derecho) I de R se llama `nil-ideal` si todos sus elementos son nilpotentes.

3.2.6 Observación. Obviamente un ideal nilpotente es un nil-ideal. El recíproco de esta afirmación es, en general, falso.

3.2.7 Lema. Toda suma finita de nil-ideales izquierdos (derechos) de un anillo R es un nil-ideal izquierdo (derecho).

Demostración. Procedemos por inducción sobre el número k de sumandos.

Caso $k = 2$**.** Sean I, J nil-ideales de R y sean $a \in I$ y $b \in J$ arbitrarios. Dado que a es nilpotente, existe $m \in \mathbb{N}$ tal que $a^m = 0$. No es difícil verificar que $(a+b)^m \in J$. Dado que J es nil-ideal, se verifica que $(a+b)^m$ es nilpotente y, por lo tanto, existe $n \in \mathbb{N}$ tal que $(a+b)^{mn} = ((a+b)^m)^n = 0$, lo cual demuestra que $I + J$ es nil-ideal.

El resto de la prueba es inmediato. □

3.3 Ejercicios

(1) Sean R un anillo conmutativo y G un grupo finito. Defina en RG la siguiente multiplicación por escalar:

$$r\Big(\sum_{g\in G} a(g)g\Big) = \sum_{g\in G}(ra(g))g,$$

con $r \in R$. Demuestre que RG es un R-módulo.

(2) Determine las tablas de las operaciones del anillo $\mathbb{Z}_3G$, siendo G un grupo cíclico con dos elementos. ¿Es $\mathbb{Z}_3G$, como anillo, isomorfo a $\mathbb{Z}_9$?

(3) Sea $n \in \mathbb{N}$. Demuestre que

   (*a*) $[a] \in \mathbb{Z}_n$ es un divisor de cero si y solo si $\text{mcd}(a, n) \neq 1$.

   (*b*) Si n es un número primo, entonces $\mathbb{Z}_n$ es un dominio entero.

   (*c*) $U(\mathbb{Z}_n) = \{[a] \mid [a] \in \mathbb{Z}_n \text{ y } \text{mcd}(a, n) = 1\}$.

   (*d*) Si n es un número primo, entonces $\mathbb{Z}_n$ es un cuerpo.

(4) Sea R un anillo. Demuestre que las siguientes afirmaciones son equivalentes:

   (*a*) R no tiene divisores de cero.

   (*b*) $(R \setminus \{0\}, \cdot)$ es un semigrupo.

   (*c*) Elementos diferentes de cero en R son cancelables. Es decir, si $0 \neq r \in R$ y $ra = rb$, entonces $a = b$ (similar a la derecha).

(5) Demuestre que el conjunto

$$I := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \; a, b \in \mathbb{R} \right\}$$

   es un ideal izquierdo de $\text{Mat}(2, \mathbb{R})$.

(6) Sea R un anillo y P un ideal de R. Demuestre que P es un ideal primo si y solo si R/P es un anillo primo.

CAPÍTULO 4

ANILLOS CONMUTATIVOS

4.1 Divisibilidad, elementos primos y elementos irreducibles

En esta sección presentamos una extensión de la divisibilidad en $\mathbb{Z}$ a un dominio entero cualquiera. Esta definición está expresada en términos de contenencia de ideales principales.

A lo largo de esta sección, R denota siempre un dominio entero. Es decir, R es un anillo conmutativo sin divisores de cero.

4.1.1 Definición. Sean $a, b \in R$.

(1) Se dice que a es un `divisor` de b, notado $a \mid b$, si existe $c \in R$ tal que $b = ac$.

(2) Diremos que a y b son `asociados`, notado $a \sim b$, si existe $c \in U(R)$ tal que $a = cb$.

Se verifica que $\sim$ es una relación de equivalencia sobre R.

4.1.2 Ejemplos. (1) En $\mathbb{Z}$ dos elementos a y b son asociados si y solo si $a = \pm b$.

(2) Si R es un cuerpo, entonces para todo $a, b \in R^\times$ se verifica que $a \sim b$.

4.1.3 Lema. (Propiedades de la divisibilidad) Sean a, b, c, d, b_1, $b_2 \ldots$, $b_n \in R$.

(1) $a \mid 0$, $1 \mid a$, $a \mid a$ y $0 \mid a$ si y solo si $a = 0$.

(2) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

(3) Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.

(4) Si $a \mid b_1, \ldots a \mid b_n$, entonces $a \mid \sum_{j=1}^{n} x_j b_j$ para todo $x_j \in R$.

(5) Si $a \mid b$, entonces para toda unidad x se verifica que $ax \mid b$.

(6) $a \sim b$ si y solo si $a \mid b$ y $b \mid a$.

(7) Si $a \sim b$, $c \sim d$ y $a \mid c$, entonces $b \mid d$.

DEMOSTRACIÓN. Se deja como ejercicio. □

El siguiente resultado prueba que la relación de divisibilidad carece de interés cuando se involucran unidades de R.

4.1.4 Lema. Sea $a \in R$. Las siguientes afirmaciones son equivalentes:

(1) $a \in U(R)$.

(2) $a \mid 1$.

(3) $a \sim 1$.

(4) $a \mid x$ para todo $x \in R$.

DEMOSTRACIÓN. Se deja como ejercicio. □

4.1.5 Teorema. Sean $a, b \in R$. Entonces

(1) $a \mid b$ si y solo si $(a) \supseteq (b)$.

(2) $a \sim b$ si y solo si $(a) = (b)$.

(3) $a \in U(R)$ si y solo si $(a) = R$.

DEMOSTRACIÓN. (1) $a \mid b \Leftrightarrow b \in Ra \Leftrightarrow (b) = Rb \subseteq Ra = (a)$.

(2) Se sigue de (a).

(3) Se sigue del lema anterior y de (b). En efecto,

$$a \in U(R) \Leftrightarrow a \sim 1 \Leftrightarrow (a) = (1) = R.$$

□

4.1.6 Definición. Sea $p \in R$ con $p \neq 0$ y $p \notin U(R)$.

(1) Decimos que p es un `elemento primo` si de $p \mid ab$ para $a, b \in R$ se sigue que $p \mid a$ o $p \mid b$.

(2) Se dice que p es `irreducible` si de $p = ab$ para $a, b \in R$ se sigue que a o b es una unidad.

4.1.7 Ejemplos. (1) El polinomio $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible.

(2) El polinomio $f = x^3 - 1 \in \mathbb{Z}[x]$ no es irreducible, ya que f puede factorizarse en la forma $f = (x-1)(x^2+x+1)$ y los factores de f no son unidades en $\mathbb{Z}[x]$.

(3) En $\mathbb{Z}$ todo número primo es un elemento primo y además irreducible.

4.1.8 Teorema. (1) Todo elemento primo es irreducible.

(2) Sea $p \in R$ irreducible. Si $a \sim p$, entonces a es irreducible.

(3) Sea $p \in R$ un elemento primo. Si $a \sim p$, entonces a es un elemento primo.

Demostración. (1) Sea $p \in R$ un elemento primo y supongamos que $p = ab$ con $a, b \in R$. Dado que $p \mid p = ab$, se sigue que $p \mid a$ o $p \mid b$.

Sin perder generalidad supongamos que $p \mid a$. Es decir, existe $r \in R$ tal que $a = pr$. En consecuencia, $p = ab = prb$ y se tiene que $p(1 - rb) = 0$. Por lo tanto, $1 - rb = 0$ o equivalentemente $rb = 1$. Esto demuestra que $b \in U(R)$.

(2) - (3) Se siguen del lema 4.1.3 (7). □

4.1.9 Definición. Un anillo conmutativo R se denomina `normado` si existe una función

$$N : R \longrightarrow \mathbb{N},$$

tal que para todo $x, y \in R$ se verifican

(1) $N(xy) = N(x)N(y)$.

(2) $N(x) = 0$ si y solo si $x \mid 0$.

(3) $N(x) = 1$ si y solo si $x \in U(R)$.

4.1.10 Ejemplo. Sea $1 \neq n \in \mathbb{N}$, el cual no es un cuadrado en $\mathbb{Z}$ y sea

$$\mathbb{Z}[\sqrt{n}] := \{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Se verifica que $\mathbb{Z}[\sqrt{n}]$ es un subanillo de $\mathbb{C}$ y que $N : \mathbb{Z}[\sqrt{n}] \longrightarrow \mathbb{N}$ definida por

$$N(x + y\sqrt{n}) = |x^2 - ny^2|$$

es una norma sobre $\mathbb{Z}[\sqrt{n}]$.

4.1.11 Ejemplo. Sea $1 \neq n \in \mathbb{N}$, el cual no es un cuadrado en $\mathbb{Z}$ y sea

$$\mathbb{Z}[\mathrm{i}\sqrt{n}] := \{x + y\mathrm{i}\sqrt{n} \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Se verifica que $\mathbb{Z}[\mathrm{i}\sqrt{n}]$ es un subanillo de $\mathbb{C}$ y que $N : \mathbb{Z}[\mathrm{i}\sqrt{n}] \longrightarrow \mathbb{N}$ definida por

$$N(x + y\mathrm{i}\sqrt{n}) = x^2 + ny^2$$

es una norma sobre $\mathbb{Z}[\mathrm{i}\sqrt{n}]$.

En el siguiente ejemplo se muestra que no siempre se verifica el recíproco de la afirmación (1) del teorema anterior. Es decir, en general no todo elemento irreducible es un elemento primo.

4.1.12 Ejemplo. Del ejemplo anterior se sigue que $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ es un anillo normado. Por otro lado, dado que $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ es un subanillo de $\mathbb{C}$, se verifica que $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ es un dominio entero.

Se verifica que $U(\mathbb{Z}[\mathrm{i}\sqrt{5}]) = \{1, -1\}$. En efecto, sea $a = x + y\mathrm{i}\sqrt{5} \in U(\mathbb{Z}[\mathrm{i}\sqrt{5}])$. Entonces existe $b \in \mathbb{Z}[\mathrm{i}\sqrt{5}]$ tal que $ab = 1$ y se sigue que

$$1 = N(1) = N(ab) = N(x + y\mathrm{i}\sqrt{5})N(b).$$

Por lo tanto, la única opción es que $N(x + y\mathrm{i}\sqrt{5}) = 1$ y se tiene que $x = \pm 1$ y $y = 0$.

Demostramos que 3 es un elemento irreducible de $\mathbb{Z}[\mathrm{i}\sqrt{5}]$. Supongamos que $3 = ab$ y que $a, b \notin U(\mathbb{Z}[\mathrm{i}\sqrt{5}])$. Es decir, $N(a) \neq 1$, $N(b) \neq 1$. Dado que

$$9 = N(3) = N(ab) = N(a)N(b),$$

solo permanece libre la opción

$$N(a) = N(b) = 3.$$

Sea $a = x + y\mathrm{i}\sqrt{5}$ con $x, y \in \mathbb{Z}$. Entonces $x^2 + 5y^2 = 3$ y se sigue que $y = 0$ y $x^2 = \pm 3$, lo cual no es posible.

Demostramos que 3 no es un elemento primo de $\mathbb{Z}[\mathrm{i}\sqrt{5}]$. Sean $a = 2 + \mathrm{i}\sqrt{5}$ y $b = 2 - \mathrm{i}\sqrt{5}$. Note que $ab = 9$ y que $3 \mid ab$. Si $3 \mid a$, entonces existe $r \in \mathbb{Z}[\mathrm{i}\sqrt{5}]$ tal que $a = 3r$. Por lo tanto,

$$9 = N(a) = 9N(r)$$

y se tendría que $N(r) = 1$. Es decir, $r = \pm 1$ con lo cual $a = \pm 3$, una contradicción. Esto demuestra que $3 \nmid a$. Similar se demuestra que $3 \nmid b$.

En el siguiente teorema expresamos en términos de ideales los conceptos de divisibilidad, primalidad, irreducibilidad, unidad y ser elementos asociados.

4.1.13 Teorema. Sea $p \in R$.

(1) p es un elemento primo si y solo si (p) es un ideal primo.

(2) p es irreducible si y solo si (p) es un ideal maximal en el conjunto de los ideales principales de R, distintos de R. Es decir, si definimos

$$\mathcal{M} := \{(a) \mid a \in R,\ (a) \neq R\},$$

entonces p es irreducible en R si y solo si (p) es maximal en $\mathcal{M}$.

DEMOSTRACIÓN. (1) Sea p un elemento primo. Entonces $p \notin U(R)$ y se tiene que $(p) \neq R$. Sean $a, b \in R$ y supongamos que $ab \in (p)$. Entonces $ab = pr$ para algún $r \in R$ y se sigue que $p \mid ab$. Entonces $p \mid a$ o $p \mid b$ y así $a \in (p)$ o $b \in (p)$.

Recíprocamente, sea (p) un ideal primo y supongamos que $p \mid ab$ para $a, b \in R$. Entonces $ab \in (p)$ y se sigue que $a \in (p)$ o $b \in (p)$. Es decir, $p \mid a$ o $p \mid b$.

(2) Sea p irreducible y supongamos que $(p) \subseteq (a)$ para $(a) \in \mathcal{M}$. Entonces $p = ar$ para algún $r \in R$. En consecuencia, $a \in U(R)$ o $r \in U(R)$. Si $a \in U(R)$, entonces $(a) = R$ y si $r \in U(R)$, de ahí que $(p) = (ra) = (a)$.

Recíprocamente, sea (p) un ideal maximal en $\mathcal{M}$ y supongamos que $p = ab$ con $a, b \in R$. Supongamos además que $a \notin U(R)$. Entonces $(a) \neq R$. De $p = ab$ se sigue que $(p) \subseteq (a)$. Por lo tanto, de la maximalidad de (p) se sigue que $(p) = (a)$. Es decir, $a = pr$ para algún $r \in R$. En consecuencia, $p = ab = prb$ y se tiene que $p(1 - rb) = 0$. Esto es $b \in U(R)$ y se tiene la conclusión. □

4.1.14 Corolario. Si R es además un anillo de ideales principales, entonces

(1) $p \in R$ es un elemento primo si y solo si p es irreducible.

(2) Un ideal no nulo (p) es maximal si y solo si (p) es un ideal primo.

(3) Si $p \in R$ es irreducible, entonces $R/(p)$ es un cuerpo.

DEMOSTRACIÓN. (1) En el teorema 4.1.8 (1) se demostró que todo elemento primo es irreducible.

Recíprocamente, sea $p \in R$ irreducible. Del teorema anterior se sigue que (p) es un ideal maximal y del teorema 3.1.13 se tiene que todo ideal maximal es un ideal primo. Es decir, (p) es un ideal primo. Del teorema anterior se sigue la primalidad de p.

(2) En el teorema 3.1.13 se demostró que todo ideal maximal es un ideal primo.

Recíprocamente, sea $(p) \neq \{0\}$ un ideal primo. Del teorema anterior se sigue que p es un elemento primo. Aplicando nuevamente el teorema 4.1.8 (1) se tiene que p es irreducible y del teorema anterior se concluye que (p) es un ideal maximal.

(3) Si $p \in R$ es irreducible, entonces (p) es maximal. Del teorema 3.1.3 se sigue que $R/(p)$ es un cuerpo. □

Consideramos ahora dos criterios para determinar la irreducibilidad de elementos del anillo de polinomios.

4.1.15 Definición. Sea R un dominio entero.

(1) Decimos que $a_1, \ldots, a_n \in R$ son `primos relativos` si el conjunto de los divisores comunes de $a_1, \ldots, a_n$ solamente tiene como elementos unidades de R.

(2) $f = \sum_{j=0}^{n} a_j x^j \in R[x]$ se denomina `primitivo` si $a_0, a_1, \ldots, a_n$ son primos relativos en R.

4.1.16 Ejemplos. Sea R un dominio entero.

(1) Todo polinomio mónico en $R[x]$ es primitivo.

(2) Si R es un cuerpo, entonces todo $0 \neq f \in R[x]$ es primitivo.

(3) $f = 3x^3 + 2x + 7 \in \mathbb{Z}[x]$ es primitivo.

4.1.17 Teorema. (Criterio de irreducibilidad de Eisenstein) Sean R un dominio entero, $f \in R[x]$, digamos $f = \sum_{i=0}^{n} a_i x^i$ con $n > 0$ y p un elemento primo de R tal que

(1) $p \mid a_j$ para todo $j = 0, \ldots, n-1$

(2) $p \nmid a_n$

(3) $p^2 \nmid a_0$

Si f es primitivo, entonces f es irreducible en $R[x]$.

Demostración. Supongamos que $f = gh$ con $g, h \in R[x]$ dados por $g = \sum_{i=0}^{k} b_i x^i$ y $h = \sum_{i=0}^{m} c_i x^i$ con $b_k \neq 0$ y $c_m \neq 0$. Entonces $a_0 = b_0 c_0$. Dado que $p \mid a_0$, pero $p^2 \nmid a_0$ se sigue que $p \nmid b_0$ o $p \nmid c_0$.

Sin perder generalidad, supongamos que $p \mid b_0$ y $p \nmid c_0$. Sea b_j el primer coeficiente de g que no es divisible por p y considere

$$a_j = \underbrace{b_j c_0}_{p\nmid} + \underbrace{b_{j-1}c_1 \cdots b_0 c_j}_{p\mid}, \quad (\text{para } i > m \text{ se tiene que } c_i = 0).$$

Entonces $p \nmid a_j$. Por hipótesis $j = n$ y es claro que $j \leq k \leq n$. Entonces $k = n$ y se tiene que

$$\operatorname{grad}(g) = n = \operatorname{grad}(f).$$

Dado que $f = gh$, se sigue que $h \in R$. Es decir, h es un polinomio constante. Pero si $f = gh$ y f es primitivo, entonces h es una unidad en R y se tiene que f es irreducible en $R[x]$. □

4.1.18 Ejemplos. Polinomios irreducibles.

(1) $f = x^4 - 2 \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Q}[x]$.

(2) En general, $f = x^n - a \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Q}[x]$, siempre que exista un número primo p con la propiedad $p \mid a$ y $p^2 \nmid a$.

(3) $f = 2x^4 + 10x^3 + 25x + 30 \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$. Es suficiente aplicar el teorema anterior con $p = 5$.

(4) Sea p un número primo, $n > 0$ y $p \nmid m$. Entonces, aplicando el criterio de Eisenstein se verifica que el polinomio $f = x^n - pm \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

(5) Sea p un número primo. Definimos el `polinomio de partición del círculo`, notado con Φ_p, de la siguiente manera:

$$\Phi_p := \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

Para todo primo p se verifica que Φ_p es irreducible en $\mathbb{Q}[x]$. Para demostrarlo consideremos el endomorfismo π de $\mathbb{Q}[x]$ (garantizado por el teorema A.2.1) con $\pi|_{\mathbb{Q}} = I_{\mathbb{Q}}$ y $\pi(x) = x + 1$. Note que π es además un automorfismo. En efecto, la inversa de π está dada por la función ρ, con $\rho|_{\mathbb{Q}} = I_{\mathbb{Q}}$ y $\rho(x) = x - 1$.

Usando la propiedad universal del cuerpo cociente podemos extender a π hasta un endomorfismo $\overline{\pi}$ de $\mathbb{Q}(x)$. Se sigue entonces que

$$\begin{aligned}
\pi(\Phi_p) &= \overline{\pi}(\Phi_p) \\
&= \frac{(x+1)^p - 1}{(x+1) - 1} \\
&= \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x + \binom{p}{p} - 1}{x} \\
&= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}.
\end{aligned}$$

Se verifica que $p \mid \binom{p}{j}$ para $j = 1, \ldots, p-1$ y $p^2 \nmid \binom{p}{1}$. Aplicando el criterio de Eisenstein se tiene que $\pi(\Phi_p)$ es irreducible en $\mathbb{Q}[x]$. Por lo tanto, Φ_p es irreducible en $\mathbb{Q}[x]$.

4.1.19 Teorema. (Reducción) Sean R, S dominios enteros y $\varphi : R \longrightarrow S$ un homomorfismo con $\varphi(1) = 1$. Este homomorfismo puede extenderse a otro homomorfismo $\hat{\varphi} : R[x] \longrightarrow S[x]$ mediante

$$\hat{\varphi}\Big(\sum_{j=0}^{n} a_j x^j\Big) = \sum_{j=0}^{n} \varphi(a_j) x^j.$$

Sea $f = \sum_{j=0}^{n} a_j x^j \in R[x]$ primitivo con $\varphi(a_n) \neq 0$. Si $\hat{\varphi}(f)$ es no constante e irreducible en $S[x]$, entonces f es no constante e irreducible en $R[x]$.

Demostración. Supongamos que f no es irreducible en $R[x]$. Entonces existen polinomios no constantes $g, h \in R[x]$ tales que $f = gh$. Aplicando el teorema A.2.1 se verifica que $\hat{\varphi}(f) = \hat{\varphi}(g)\hat{\varphi}(h)$. Por lo tanto,

$$\operatorname{grad}(\hat{\varphi}(g)) + \operatorname{grad}(\hat{\varphi}(h)) = \operatorname{grad}(\hat{\varphi}(f)) = \operatorname{grad}(f) = \operatorname{grad}(g) + \operatorname{grad}(h)$$

se verifica que $\operatorname{grad}(\hat{\varphi}(g)) = \operatorname{grad}(g)$ y $\operatorname{grad}(\hat{\varphi}(h)) = \operatorname{grad}(h)$, lo cual contradice la irreducibilidad de $\hat{\varphi}(f)$ en $S[x]$. □

4.1.20 Ejemplos. Aplicaciones del teorema de reducción.

(1) Sea $f = x^3 + 6x^2 + 8x + 4 \in \mathbb{Z}[x]$. Note que el criterio de Eisenstein no es aplicable. Para demostrar que f es irreducible sobre $\mathbb{Z}$, consideremos la función $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_3$ definida por $\varphi(x) = [x]$. Entonces $\hat{\varphi}(f) = x^3 - x + 1$. Dado que $\hat{\varphi}(f)$ no tiene raíces en $\mathbb{Z}_3$, se tiene que este es irreducible. Aplicando el teorema de reducción se tiene que f es irreducible sobre $\mathbb{Z}$.

(2) En general es falso que si f es irreducible en $R[x]$, entonces $\hat{\varphi}(f)$ es irreducible en $S[x]$. Por ejemplo, el polinomio $f = x^2 + 1 \in \mathbb{Z}[x]$ es irreducible, pero $\hat{\varphi}(f) \in \mathbb{Z}_2[x]$ está dado por $\hat{\varphi}(f) = (x+1)^2$, el cual claramente no es irreducible.

(3) Sea $f = x^5 - x^2 + 1 \in \mathbb{Z}[x]$. Definamos nuevamente $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_2$ por $f(x) = [x]$. Entonces $\hat{\varphi}(f) = x^5 - x^2 + 1$.

Supongamos que $\hat{\varphi}(f) = gh$ con $g, h \in \mathbb{Z}_2[x]$. Diferenciamos algunos casos posibles:

`Caso 1.` $\operatorname{grad}(g) = 1$. Entonces $\hat{\varphi}(g)$ tendría una raíz en $\mathbb{Z}_2$, lo cual no es posible.

`Caso 2.` $\operatorname{grad}(g) = 2$. Entonces existen las opciones

$$g = x^2 + x + 1,\ g = x^2 + x,\ g = x^2 + 1, \quad \text{o} \quad g = x^2.$$

De estas opciones solo permanece posible $g = x^2 + x + 1$, ya que para las otras 0 o 1 sería una raíz. Usando división con resto se tiene que

$$\hat{\varphi}(f) = (x^3 + x^2)(x^2 + x + 1) + 1.$$

Es decir, $x^2 + x + 1$ no es un divisor de $\hat{\varphi}(f)$. Por lo tanto, $\hat{\varphi}(f)$ es irreducible en $\mathbb{Z}_2[x]$ y, en consecuencia, también lo es sobre $\mathbb{Z}$.

4.2 Anillos de factorización única

4.2.1 Definición. Sea R un dominio entero.

(1) R tiene la propiedad $(A) \Leftrightarrow$ Para todo $0 \neq a \notin U(R)$ existen elementos irreducibles $q_1, \ldots, q_r \in R$ tales que $a = q_1 \cdots q_r$.

(2) R tiene la propiedad $(A') \Leftrightarrow$ Para todo $0 \neq a \notin U(R)$ existen elementos primos $p_1, \ldots, p_r \in R$ tales que $a = p_1 \cdots p_r$.

(3) R tiene la propiedad $(B) \Leftrightarrow$ Si $q_1, \ldots, q_r$ y $q'_1, \ldots, q'_s$ son elementos irreducibles de R con $q_1 \cdots q_r = q'_1 \cdots q'_s$, entonces $r = s$ y existe $\pi \in \mathrm{Sym}(r)$ tal que $q'_j \sim q_{\pi(j)}$. Es decir, q'_j y $q_{\pi(j)}$ son asociados.

(4) R tiene la propiedad $(C) \Leftrightarrow$ Todo elemento irreducible de R es un elemento primo de R.

4.2.2 Teorema. En un dominio entero R, las siguientes afirmaciones son equivalentes:

(1) R tiene las propiedades (A) y (B).

(2) R tiene las propiedades (A) y (C).

(3) R tiene la propiedad (A').

Demostración. (1) $\Rightarrow$ (2). Es suficiente demostrar que todo elemento irreducible es un elemento primo.

Sea $q \in R$ un elemento irreducible y supongamos que $q \mid ab$ con $a, b \in R$. Entonces existe $c \in R$ tal que

$$ab = qc. \tag{4.1}$$

`Caso 1.` Si $a \in U(R)$, entonces $b = a^{-1}qc$ y se tiene que $q \mid b$.

`Caso 2.` Si $b \in U(R)$, entonces se tiene que $q \mid a$.

`Caso 3.` Si $c \in U(R)$, entonces $q = abc^{-1}$. Dado que por hipótesis q es irreducible, se sigue que $a \in U(R)$ o $bc^{-1} \in U(R)$. La primera opción se consideró en el caso 1 y si $bc^{-1} \in U(R)$, entonces $b \in U(R)$, lo cual se consideró en el caso 2.

`Caso 4.` Si $c = 0$, entonces $a = 0$ o $b = 0$ y se tiene que $q \mid a$ o $q \mid b$.

Entonces podemos suponer, sin perder generalidad, que $a, b, c \notin U(R)$ y que $c \neq 0$. Aplicando la hipótesis (A) tenemos que

$$\begin{aligned} a &= q_1 \cdots q_m \\ b &= r_1 \cdots r_n \\ c &= t_1 \cdots t_s \end{aligned}$$

con $q_j, r_i, t_k \in R$. Reemplazando en (4.1) se tiene que

$$q_1 \cdots q_m r_1 \cdots r_n = q t_1 \cdots t_s.$$

Aplicando la hipótesis (B) se tiene que $q \sim q_{j_0}$ para algún $j_0 \in \{1, \ldots, m\}$ o $q \sim r_{i_0}$ para algún $i_0 \in \{1, \ldots, n\}$. En consecuencia, $q \mid a$ o $q \mid b$. Esto demuestra que q es un elemento primo de R.

$(2) \Rightarrow (3)$. Evidente.

$(3) \Rightarrow (1)$. Dado que todo elemento primo de R es irreducible (lema 4.1.8 (1)), se tiene que de (A') podemos inferir (A).

Demostramos inicialmente que de (A') se sigue que todo elemento de R que sea irreducible es un elemento primo. Para ello, sea $q \in R$ irreducible. De (A') se sigue que

$$q = p_1 \cdots p_m,$$

con $p_j \in R$ elemento primo. Dado que q es irreducible y $p_1 \notin U(R)$, se sigue que $p_2 \cdots p_m \in U(R)$. En consecuencia, para cada $j \in \{2, \ldots, m\}$ se verifica que $p_j \mid 1$. Por lo tanto, $m = 1$ y se tiene que $q = p_1$.

En lo que sigue demostramos que R tiene la propiedad (B). Supongamos que

$$q_1 \cdots q_r = q'_1 \cdots q'_s$$

con $q_1, \ldots, q_r$ y $q'_1, \ldots, q'_s$ elementos irreducibles de R, por lo tanto, elementos primos. Entonces

$$q'_1 \mid q_1 \cdots q_r$$

y, por consiguiente, $q'_1 \mid q_{j_0}$ para algún $j_0 \in \{1, \ldots, r\}$. Es decir, existe $a \in R$ tal que $q_{j_0} = q'_1 a$. Dado que q_{j_0} es irreducible, se sigue que $q'_1 \in U(R)$ o $a \in U(R)$. Note que la primera opción no es posible, por lo tanto $a \in U(R)$. Esto trae como consecuencia que $q_{j_0} \sim q'_1$. Dado que

R es conmutativo, sin perder generalidad, supongamos que $q_1 = q_1' a$. Dado que en R no hay divisores de cero tenemos que

$$aq_2 \cdots q_r = q_2' \cdots q_s'.$$

El resto se sigue por inducción matemática. □

4.2.3 Definición. Un dominio entero R se denomina un dominio de `factorización única` o de `factorización prima` o simplemente un DFU-anillo si se verifica alguna, por lo tanto todas, de las propiedades del teorema 4.2.2. También es usual llamar a R un anillo `factorial` o también un anillo `gaussiano`.

4.2.4 Teorema. Sea R un dominio entero con elemento identidad. Si R es noetheriano, entonces R tiene la propiedad (A).

Demostración. Demostramos que si R es un dominio entero y R no tiene la propiedad (A), entonces R no es noetheriano. Para ello, sea $0 \neq a \notin U(R)$ y supongamos que a no es producto de elementos irreducibles de R. Entonces a no es irreducible y se tiene que existen $a_1, b_1 \notin U(R)$ tales que $a = a_1 b_1$. Si a_1 y b_1 pudiesen expresarse como productos de irreducibles, entonces a también lo sería.

Supongamos entonces, sin perder generalidad, que a_1 está en la misma situación que a. Es decir, $0 \neq a_1 \notin U(R)$ y a_1 no es producto de elementos irreducibles de R. Dado que $a_1 \mid a$, se tiene que $(a) \subseteq (a_1)$. Demostramos que $a_1 \notin (a)$. En efecto, si $a_1 \in (a)$, entonces $a_1 = ar$ para algún $r \in R$. Entonces $a_1 = a_1 b_1 r$ y se tendría que

$$\underbrace{a_1}_{\neq 0}(1 - b_1 r) = 0.$$

Por lo tanto, $b_1 r = 1$ y se tendría que $b_1 \in U(R)$, lo cual es una contradicción. Esto implica que $(a) \subset (a_1)$. Repitiendo este procedimiento tenemos una cadena ascendente de ideales principales

$$(a) \subset (a_1) \subset (a_2) \subset \cdots,$$

que no se estaciona. Esto demuestra que R no es noetheriano. □

4.2.5 Corolario. Si R es un dominio entero y, además, un anillo de ideales principales, entonces R es un DFU-anillo.

Demostración. Del corolario 4.1.14 (1) se sigue que R tiene la propiedad (C). Dado que todo anillo de ideales principales es noetheriano, del teorema anterior se tiene que R tiene la propiedad (A). Por lo tanto, R es un DFU-anillo. □

4.2.6 Ejemplos. (1) $\mathbb{Z}$ y $K[x]$ son anillos de factorización única.

(2) $\mathbb{Z}[i\sqrt{5}]$ no es un anillo de factorización única. Note que $3, 2+i\sqrt{5}$ y $2-i\sqrt{5}$ son elementos no asociados e irreducibles. En efecto, la no asociatividad es clara. Por otro lado, sea $w \in \{3, 2+i\sqrt{5}, 2-i\sqrt{5}\}$ y supongamos que $w = xy$. Entonces, usando la norma definida en el ejemplo 4.1.12 se sigue que

$$9 = N(x)N(y),$$

con $N(x) > 0$. En consecuencia, $N(x) \in \{1, 3, 9\}$.

Caso 1. Si $N(x) = 1$, entonces $x \in U(R)$.

Caso 2. Si $N(x) = 9$, entonces $N(y) = 1$ y se sigue que $y \in U(R)$.

Caso 3. Si $N(x) = 3 = a^2 + 5b^2$ con $a, b \in \mathbb{Z}$, entonces se tiene una contradicción.

Note finalmente que

$$9 = 3 \cdot 3 = (2+i\sqrt{5})(2-i\sqrt{5}).$$

4.3 Polinomios sobre anillos de factorización única

4.3.1 Lema. Sea R un dominio entero. Si p es un elemento primo en R, entonces p es un elemento primo en $R[x]$.

DEMOSTRACIÓN. Del teorema 4.1.13 se sigue que p es un elemento primo de R si y solo si $p \neq 0$ y (p) es un ideal primo en R. Por lo tanto, es suficiente demostrar que $pR[x]$ es un ideal primo en $R[x]$. Para ello, sea $\bar{R} := R/(p)$ y definamos

$$\tau : R[x] \longrightarrow \bar{R}[x]$$

mediante

$$\tau\Big(\sum_{j=0}^{n} a_j x^j\Big) = \sum_{j=0}^{n} (a_j + (p))x^j.$$

Se verifica que τ es un epimorfismo, cuyo núcleo es $\ker(\tau) = pR[x]$. Aplicando el primer teorema de isomorfía se tiene que

$$R[x]/pR[x] = R[x]/\ker(\tau) \cong \mathrm{Im}(\tau) = \bar{R}[x].$$

Dado que (p) es un ideal primo, del teorema 3.1.8 se sigue que $\bar{R}$ es un dominio entero y, en consecuencia, $\bar{R}[x]$ también lo es. Aplicando nuevamente el teorema 3.1.8 se sigue que $pR[x]$ es un ideal primo de $R[x]$. Aplicando el teorema 4.1.13 se tiene la conclusión. □

4.3.2 Teorema. Sea R un dominio entero.

(1) Todo polinomio irreducible $f \in R[x]$ con $\text{grad}(f) > 0$ es primitivo.

(2) Sea $K = Q(R)$. Si $f \in R[x]$ es primitivo e irreducible en $K[x]$, entonces f es irreducible en $R[x]$.

DEMOSTRACIÓN. (1) Sea a un divisor común de los coeficientes de f. Entonces $f = ag$ para algún $g \in R[x]$ y se verifica que

$$0 < \text{grad}(f) = \text{grad}(g).$$

Es decir, g no es un polinomio constante y, por lo tanto, del teorema A.1.9 (d) se sigue que g no es una unidad en $R[x]$. Dado que f es irreducible, se sigue que $a \in U(R[x])$ y, por lo tanto, $a \in U(R)$. En conclusión, f es primitivo.

(2) Supongamos que $f = gh$ con $g, h \in R[x]$. Por hipótesis se tiene que f es irreducible en $K[x]$, por lo tanto g o h es una unidad en $K[x]$. Sin perder generalidad, supongamos que $g \in U(K[x])$. Usando nuevamente el teorema A.1.9 (d) se tiene que $g \in R[x] \cap K = R$. Entonces g es un divisor de los coeficientes de f, pero por hipótesis f es primitivo, por lo tanto $g \in U(R[x])$ con lo cual se demuestra la afirmación. □

En el teorema anterior (2), es importante la hipótesis $f \in R[x]$ primitivo, ya que en general la afirmación puede ser falsa. Por ejemplo, el polinomio $2x \in \mathbb{Q}[x]$ es irreducible, pero no lo es en $\mathbb{Z}[x]$.

4.3.3 Lema. (Gauss) Sean R un DFU-anillo y $f, g \in R[x]$ primitivos. Entonces fg también es primitivo.

DEMOSTRACIÓN. Supongamos que fg no es primitivo. Entonces, sin perder generalidad, podemos asumir que existe un elemento primo $p \in R$ que divide a todos los coeficientes de fg. En particular se verifica que $p \mid fg$. Del lema 4.3.1 se sigue que p es un elemento primo en $R[x]$. Por lo tanto, $p \mid f$ o $p \mid g$, lo cual es una contradicción, ya que por hipótesis f y g son primitivos. □

4.3.4 Teorema. Sea R un DFU-anillo y $K := Q(R)$.

(1) Para todo $0 \neq g \in K[x]$ existe $a \in K^\times$ tal que $ag \in R[x]$ es primitivo.

(2) Si $f, g \in R[x]$, g primitivo y $f = ag$ con $a \in K$, entonces, $a \in R$.

(3) Si $0 \neq f \in K[x]$, entonces, existen $b \in R$ y $g \in R[x]$ primitivo tales que $f = bg$.

DEMOSTRACIÓN. (1) Sea $g = \sum_{j=0}^{n} a_j x^j$ y para todo $j \in \{0, \ldots, n\}$ sean $a_j := \frac{r_j}{s_j}$ con $r_j, s_j \in R$. Si definimos

$$s := s_0 s_1 \cdots s_n,$$

entonces, $0 \neq sg \in R[x]$. Sea ahora d el máximo común divisor de los coeficientes de sg en R. Si definimos $a := \frac{s}{d} \in K$, entonces, $a \in K^\times$, $ag \in R[x]$ y ag es primitivo.

(2) Dado $a \in K$, se tiene que existen $r, s \in R$ primos relativos con $a = \frac{r}{s}$. Supongamos además que $a \notin R$. Entonces s no es una unidad en R. Es decir, existe un elemento primo $p \in R$ con $p \mid s$. Por hipótesis se tiene que g es primitivo, por tanto p no divide todos los coeficientes de g.

Por otro lado, $f = ag = \frac{r}{s}g$, por lo tanto $sf = rg$ y se cumple que $p \mid s$, pero $p \nmid r$. Entonces $p \mid g$. Es decir, p divide todos los coeficientes de g, lo cual es contradictorio, ya que g es primitivo. Por lo tanto, $a \in R$.

(3) De (1) se sigue que existe $a \in K^\times$ tal que $af \in R[x]$ es primitivo. Note que $f = a^{-1}(af)$, con $f, af \in R[x]$. El resto se sigue de (2) con af en lugar de g. □

4.3.5 Ejemplos. Ilustración del teorema anterior.

(1) Si $f = 6x^3 + 8x^2 + 10 \in \mathbb{Z}[x]$, entonces, $f = 2g$ con $g = 3x^3 + 4x^2 + 5 \in \mathbb{Z}[x]$ primitivo.

(2) Si $f = \frac{3}{2}x^4 + \frac{1}{4}x^3 + 2x - \frac{7}{5} \in \mathbb{Q}[x]$, entonces, $20f = g$, donde g es el polinomio $30x^4 + 5x^3 + 40x + 28 \in \mathbb{Z}[x]$ primitivo.

En el siguiente resultado se presenta la versión recíproca del teorema 4.3.2 (2).

4.3.6 Teorema. Sea R un DFU-anillo, $K := Q(R)$ y $f \in R[x]$ no constante.

(1) Si f es primitivo, $g \in R[x]$ no constante y $f \mid g$ en $K[x]$, entonces $f \mid g$ en $R[x]$.

(2) Si f es irreducible en $R[x]$, entonces f también es irreducible en $K[x]$.

(3) Si f es primitivo y f es un elemento primo en $K[x]$, entonces f es un elemento primo en $R[x]$.

Demostración. (1) Sea $g = fh$ con $g, h \in K[x]$. Del teorema anterior (1) se sigue que existe $a \in K^\times$ tal que $h_1 := ah \in R[x]$ es primitivo. Por lo tanto,

$$g = \frac{1}{a}(fh_1).$$

Dado que f y h_1 son primitivos, del lema de Gauss 4.3.3 se sigue que $fh_1 \in R[x]$ es primitivo. Usando ahora el teorema 4.3.4 (2) se tiene que $\frac{1}{a} \in R$, por lo tanto $f \mid g$ en $R[x]$.

(2) Sea $g \in K[x]$ un divisor de f. Usando el teorema 4.3.4 (1) se sigue que existe $a \in K^\times$ tal que $g_1 := ag \in R[x]$ es primitivo. Dado que $g \mid f$ en $K[x]$, se verifica que $g_1 \mid f$ en $K[x]$. Dado que g_1 es primitivo, usando (1) se tiene que $g_1 \mid f$ en $R[x]$. La irreducibilidad de f en $R[x]$ implica que $g_1 \in U(R[x])$ o que g_1 es asociado con f.

Si $g_1 \in U(R[x])$, entonces dado que $g_1 = ag$ con $a \in K^\times$, se tiene que $g \in K$. Es decir, $g \in K$.

Si g_1 es asociado con f, entonces $f = bg$ para algún $b \in K$ y se tiene que f es irreducible en $K[x]$.

(3) Sean $g, h \in R[x]$ con $f \mid gh$. Dado que f es un elemento primo en $K[x]$, se sigue que $f \mid g$ o $f \mid h$ en $K[x]$. Usando (1) se tiene que $f \mid g$ o $f \mid h$ en $R[x]$. □

4.3.7 Teorema. (Gauss) Si R es un DFU-anillo, entonces $R[x]$ también es un DFU-anillo.

Demostración. Demostramos que $R[x]$ satisface la propiedad (A'). Es decir, demostramos que todo $0 \neq f \in R[x]$, que no es una unidad, puede expresarse como producto de elementos primos. Para ello procedemos por inducción matemática sobre el grado de f.

Si $\text{grad}(f) = 0$, entonces $f \in R$. Dado que f no es una unidad y R es un DFU-anillo, se sigue que f es producto de elementos primos de R. Del lema 4.3.1 se sigue que f es producto de elementos primos de $R[x]$.

`Hipótesis inductiva.` Supongamos que todo polinomio con grado menor o igual al grado de f satisface la afirmación.

`Conclusión.` Del teorema 4.3.4 (3) se tiene que existen $b \in R$ y $g \in R[x]$ primitivo tales que $f = bg$. Dado que R es un DFU-anillo, se sigue que $b \in U(R)$ o b es el producto de elementos primos de R. Usando nuevamente el lema 4.3.1 se sigue que $b \in U(R[x])$ o b es el producto de elementos primos de $R[x]$.

Sea $K := Q(R)$. Entonces $K[x]$ es un anillo euclidiano y, por lo tanto, un DFU-anillo. En consecuencia g es el producto de elementos primos de $K[x]$. Sea $p \in K[x]$ un divisor primo de g. Entonces del teorema 4.3.4 (1) se sigue que si multiplicamos a p por un elemento de K podemos suponer que $p \in R[x]$ y que además es primitivo. Del teorema 4.3.6 (3) se sigue que p es un elemento primo en $R[x]$ y de 4.3.6 (1) se tiene que p divide a g en $R[x]$. Por lo tanto,

$$f = bg = bph,$$

con $h \in R[x]$. En resumen tenemos:

(1) $b \in U(R[x])$ o b es el producto de elementos primos de $R[x]$.

(2) p es un elemento primo en $K[x]$, por lo tanto $\text{grad}(p) > 0$.

(3) p es un elemento primo en $R[x]$.

(4) $\text{grad}(h) < \text{grad}(f)$, ya que $\text{grad}(p) > 0$.

Usando la hipótesis inductiva se tiene que h es producto de elementos primos de $R[x]$ con lo cual se tiene el resultado. □

4.3.8 Corolario. (Gauss) Si R es un DFU-anillo, entonces $R[x_1, \ldots, x_n]$ también es un DFU-anillo.

DEMOSTRACIÓN. Se sigue inmediatamente del teorema anterior. □

Presentamos ahora una versión más fuerte del criterio de irreducibilidad de Eisenstein.

4.3.9 Teorema. (Criterio de irreducibilidad de Eisenstein) Sean R un dominio entero, $f \in R[x]$, digamos $f = \sum_{i=0}^{n} a_i x^i$ con $n > 0$ y p un elemento primo de R tal que

(1) $p \mid a_j$ para todo $j = 0, \ldots, n-1$

(2) $p \nmid a_n$

(3) $p^2 \nmid a_0$

Entonces

(a) Si f es primitivo, entonces f es irreducible en $R[x]$.

(b) Si R es un DFU-anillo y $K = Q(R)$, entonces f es irreducible en $K[x]$.

DEMOSTRACIÓN. (a) Supongamos que $f = gh$ con $g, h \in R[x]$ dados por $g = \sum_{i=0}^{k} b_i x^i$ y $h = \sum_{i=0}^{m} c_i x^i$ con $b_k \neq 0$ y $c_m \neq 0$. Entonces $a_0 = b_0 c_0$. Dado que $p \mid a_0$ pero $p^2 \nmid a_0$ se sigue que $p \nmid b_0$ o $p \nmid c_0$.

Sin perder generalidad, supongamos que $p \mid b_0$ y $p \nmid c_0$. Sea b_j el primer coeficiente de g, que no es divisible por p y considere

$$a_j = \underbrace{b_j c_0}_{p\nmid} + \underbrace{b_{j-1} c_1 \cdots b_0 c_j}_{p|}, \quad (\text{para } i > m \text{ se tiene que } c_i = 0).$$

Entonces $p \nmid a_j$. Por hipótesis $j = n$ y es claro que $j \leq k \leq n$. Entonces $k = n$ y se tiene que

$$\operatorname{grad}(g) = n = \operatorname{grad}(f).$$

Dado que $f = gh$, se sigue que $h \in R$. Es decir, h es un polinomio constante. Pero si $f = gh$ y f es primitivo, entonces h es una unidad en R y se tiene que f es irreducible en $R[x]$.

(b) Sea $f = gh$ con g irreducible en $R[x]$ y $h \in R[x]$. Similar como en (1) se sigue que $h \in R$. Dado que g es irreducible en $R[x]$, del teorema 4.3.6 (2) se sigue que g es irreducible en $K[x]$. En consecuencia, f es irreducible en $K[x]$. □

4.4 Ejercicios

(1) Sea $\varphi : R \longrightarrow T$ un homomorfismo de anillos. ¿Bajo qué condiciones $\mathrm{Im}(\varphi)$ es un ideal de T?

(2) Sean A y B ideales de un anillo R. Definimos

$$A + B := \{x + y \mid x \in A \;\; y \in B\}$$

Demuestre que $A + B$ es un ideal de R y, además, $A \subseteq A + B$.

(3) Sea $(G, +)$ un grupo abeliano y sea $H := \mathrm{End}(G)$. Si definimos para $f, g \in \mathrm{End}(G)$ y $x \in G$,

$$(f + g)(x) := f(x) + g(x)$$

y como multiplicación en H consideramos la composición de funciones. ¿Es $(H, +, \circ)$ un anillo? En caso afirmativo, ¿tiene elemento identidad?

(4) Exhiba todos los ideales del anillo $\mathbb{Z}$.

(5) Clasifique los siguientes anillos como conmutativos, dominio entero con división, cuerpo.

$$\mathbb{Z},\ \mathbb{R}, \mathbb{C} \text{ y } \ \mathbb{Z}_8$$

(6) `Demuestre o refute.` Sea R un anillo.

(a) Para todo $x, y \in R$ se verifica que $x^2 - y^2 = (x - y)(x + y)$.

(b) Si R es un cuerpo, entonces R admite ideales no triviales.

(c) Si A es un subanillo de R y J un ideal del R, entonces $A \cap J$ es un ideal de A.

(d) Si R es un dominio entero finito, entonces R es un cuerpo.

(7) Sea R un anillo y supóngase que para cada $0 \neq x \in R$ existe un único $y \in R$ tal que $xyx = x$. Demuestre que

(a) R no tiene divisores de cero.

(b) R es un anillo con división.

(c) $yxy = y$.

(8) Sea R un anillo para el cual se verifica que $x^2 = x$ para todo $x \in R$. Demuestre que

(a) En R se verifica que $x + x = 0$ para todo $x \in R$.

(b) R es conmutativo.

(c) Si R no tiene divisores de cero, entonces $R \cong \mathbb{Z}_2$.

(9) Sea R un anillo. Un elemento $x \in R$ se denomina `idempotente` si $x^2 = x$. Demuestre que si R es un dominio entero, entonces los únicos elementos idempotentes son 0 y 1.

(10) Sea R un anillo. Demuestre que las siguientes afirmaciones son equivalentes:

- (a) R no tiene elementos nilpotentes no nulos.
- (b) Si $r \in R$ y $r^2 = 0$, entonces $r = 0$.

(11) Sea R un anillo conmutativo y sea N el conjunto de todos los elementos nilpotentes de R.

- (a) Demuestre que R/N es un anillo que no tiene elementos nilpotentes no nulos.
- (b) Demuestre que N es un ideal de R.

(12) Demuestre que si R es conmutativo y $a, b \in R$ son nilpotentes, entonces $a + b$ también lo es.

(13) Demuestre que si R es un anillo conmutativo, entonces $I := \{x \in R \mid x \text{ es nilpotente}\}$ es un ideal de R.

(14) Sea R un anillo y $a \in R$ un elemento fijo. Sea $I_a := \{x \in R \mid ax = 0\}$. ¿Es I_a un subanillo de R? ¿Es un ideal de R? Si $R = \mathrm{Mat}(2, \mathbb{R})$ y $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Halle I_a.

(15) Sea R un anillo conmutativo. Demuestre que las siguientes afirmaciones son equivalentes:

- (a) $R \neq M$ es un ideal maximal de R.
- (b) Para todo $r \in R \setminus M$ existe $x \in R$ tal que $1 - rx \in M$.

(16) Determine todos los ideales primos y maximales de $\mathbb{Z}_8$. ¿Admite $\mathbb{Z}_8$ ideales primos? ¿Tiene ideales maximales?

(17) Sea $\varphi : A \longrightarrow B$ un epimorfismo de anillos con núcleo N. Demuestre que

- (a) Si P es un ideal primo de A que contiene a N, entonces $\varphi(P)$ es un ideal primo de B.
- (b) Si P' es un ideal primo de B, entonces $\varphi^{-1}(P')$ es un ideal primo de A.

(18) Sea R un anillo conmutativo. Demuestre que las siguientes afirmaciones son equivalentes:

- (a) $R \neq M$ es un ideal maximal de R.
- (b) Para todo $r \in R \setminus M$ existe $x \in R$ tal que $1 - rx \in M$.

(19) Determine todos los ideales primos y maximales de $\mathbb{Z}_6$.

(20) ¿Existe un anillo con división con 11 elementos?

(21) Halle (si existe) un subconjunto de $\mathbb{Z}_8$ que sea un cuerpo con las operaciones restringidas a este.

(22) En la siguiente tabla se presentan ejemplos de anillos. En cada columna marque con una × si el anillo satisface la propiedad.

Anillo	$\mathbb{Z}$	$\mathbb{Z}_4$	$\mathbb{R}$	$\mathrm{Mat}(n,\mathbb{R})$	Cuaterniones
Conmutativo					
Existe un 1					
Dominio entero					
Con división					
Cuerpo					

(23) Sea R un anillo y definamos

$$\mathrm{Z}(R) \coloneqq \{r \in R \mid rx = xr,\ \forall\ x \in R\}.$$

¿Es $\mathrm{Z}(R)$ un subanillo de R? ¿Es un ideal?

(24) Demuestre que $\mathbb{Z}[x]$ no es un anillo de ideales principales.

(25) Demuestre $\mathbb{Z}[x]$ no es un anillo euclidiano.

(26) Demuestre $\mathbb{Z}[\sqrt{3}]$ es un anillo euclidiano.

(27) Sea K un cuerpo. ¿Se verifica que $K[x]$ es un anillo noetheriano?

(28) Sea R un anillo conmutativo y A un ideal de R. Definamos

$$\sqrt{A} \coloneqq \{a \in R \mid a^n \in A,\ \text{para algún } n \in \mathbb{N}\}.$$

Diremos que A es `reducido` si $\sqrt{A} = A$. Demuestre que

(a) A es un ideal de R.

(b) A es reducido si y solo si R/A no tiene elementos nilpotentes.

(c) Todo ideal primo es reducido.

(d) Para $R = \mathbb{Z}_n$, determine $N \coloneqq \sqrt{(0)}$, así como R/N.

(29) Sea K un cuerpo. Demuestre que un ideal $\langle f \rangle \neq \{0\}$ de $K[x]$ es maximal si y solo si f es irreducible sobre K.

(30) Sea K un cuerpo.

(a) Demuestre que
$$B = (x^j \mid j \in \mathbb{N}_0)$$
es una base (como K-álgebra) para $K[x]$.

(b) Demuestre que $K[x]$ no tiene divisores de cero y que $K^\times$ es el conjunto de todas las unidades de $K[x]$.

(31) Determine todas las unidades y todos los elementos primos en el anillo Gaussiano $\mathbb{Z}[i]$.

(32) Sea $\varphi : K \longrightarrow L$ un homomorfismo de cuerpos. Demuestre que φ es inyectiva o es la función idénticamente nula.

(33) Sea L un dominio entero y K un subanillo de L que tiene la estructura de cuerpo. Claramente es L un espacio vectorial sobre K. Demuestre que si la dimensión de L sobre K es finita, entonces L es un cuerpo.

`Sugerencia:` para $0 \neq a \in L$ defina la función $f_a : L \longrightarrow L$ definida por $f_a(x) = xa$.

(34) Sea R un anillo.

(a) Sea $\varnothing \neq I \subset R$. Demuestre que I es un ideal de R si y solo si I es aditivamente cerrado y para todo $r_1, r_2 \in R$ y todo $i \in I$ se verifica que $r_1 i r_2 \in I$.

(b) Demuestre que la afirmación anterior no es válida si R no tiene elemento identidad.

Sugerencia: sea K un cuerpo,
$$R = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \;\middle|\; a, b, c \in K \right\}$$
$$I = \left\{ \begin{pmatrix} 0 & x & 0 \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix} \;\middle|\; x, y \in K \right\}.$$

(35) Sea R un dominio entero. Demuestre que si toda cadena descendente de ideales
$$I_1 \supseteq I_2 \supseteq \cdots$$
se estaciona, entonces R es un cuerpo.

`Sugerencia:` para $0 \neq a \in R$ considere la cadena
$$aR \supseteq a^2R \supseteq \cdots$$

(36) Sea R un anillo. Demuestre que

(a) Si $a \in R^\times$, es decir, a es una unidad de R y $b \in R$, entonces la función

$$\varphi_{a,b} : R[x] \longrightarrow R[x]$$

definida por

$$x \longmapsto ax + b$$

es un R-automorfismo de álgebras.

(b) Si R es un dominio entero, entonces todo R-automorfismo de álgebras de $R[x]$ es de esta forma. Es decir,

$$\mathrm{Aut}_R(R[x]) = \{\varphi_{a,b} \mid a \in R^\times,\ b \in R\}.$$

Demuestre además que

$$N := \{\varphi_{1,b} \mid b \in R\}$$

es un subgrupo normal de $\mathrm{Aut}_R(R[x])$ y que los siguientes grupos son isomorfos: $N \cong (R, +)$ y $\mathrm{Aut}_R(R[x])/N \cong (R^\times, \cdot)$.

(c) Determine $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}[x])$.

(37) Sea R un anillo conmutativo.

(a) Sea P un ideal primo. Demuestre que $S := R \setminus P$ es un conjunto multiplicativamente cerrado y $0 \notin S$.

(b) Sea $S \subset R$ un conjunto multiplicativamente cerrado con $0 \notin S$. Sea P un ideal de R, el cual es maximal en el conjunto de todos los ideales de R que tienen intersección vacía con S. Demuestre que P es un ideal primo de R.

`Conclusión:` los ideales primos de R son exactamente aquellos cuyos complementos en R son conjuntos cerrados multiplicativamente y que no contienen al cero.

(38) Un anillo conmutativo se denomina `artiniano` si toda cadena descendente de ideales de R

$$I_1 \supseteq I_2 \supseteq \cdots$$

se estaciona. Demuestre que todo ideal primo de R es maximal.

(39) Demuestre que todo ideal primo de un anillo finito es maximal.

(40) Sea R un anillo conmutativo. Sea $S \subseteq R$ cerrado multiplicativamente.

(a) Sobre $R \times S$ defina la siguiente relación:

$$(r_1, s_1) \sim (r_2, s_2) \Longleftrightarrow s(r_1 s_2 - r_2 s_1) = 0, \quad \text{para algún} \quad s \in S.$$

Demuestre que $\sim$ es una relación de equivalencia. Para la clase de equivalencia $[(r, s)]$ escribiremos en lo que sigue r/s. Notaremos con $S^{-1}R$ al conjunto de todas las clases de equivalencia. Llamaremos a $S^{-1}R$ `una localización` de R mediante S.

(b) Demuestre que $S^{-1}R$ es un anillo conmutativo con respecto a las siguientes operaciones:

$$r_1/s_1 + r_2/s_2 := (r_1 s_2 + r_2 s_1)/s_1 s_2.$$
$$r_1/s_1 \cdot r_2/s_2 := r_1 r_2/s_1 s_2.$$

(c) Demuestre que la función $\varphi : R \longrightarrow S^{-1}R$ definida por

$$\varphi(r) = r/1$$

es un homomorfismo de anillos. Más aún, si $0 \notin S$ y S no tiene divisores de cero, entonces φ es un monomorfismo.

(d) Demuestre que si I es un ideal de R, entonces

$$S^{-1}I := \{i/s \mid i \in I,\ s \in S\}$$

es un ideal de $S^{-1}R$. Se verifica además que $S^{-1}I = S^{-1}R$ si y solo si $S \cap I \neq \varnothing$.

(e) Demuestre que todos los ideales de $S^{-1}R$ tienen la forma $S^{-1}I$ para algún ideal I de R.

`Sugerencia:` demuestre que para un ideal J de $S^{-1}R$ se verifica que

$$J = S^{-1}(\varphi^{-1}(J)),$$

donde $\varphi^{-1}(J)$ es un ideal de R.

(f) Si en particular $S = R \setminus \{0\}$, entonces la localización $S^{-1}R$ de R es un cuerpo, este no es más que el cuerpo cociente de R.

(41) Sea R un anillo euclidiano con respecto a una función $\varphi : R \longrightarrow \mathbb{N}_0$. Demuestre que el conjunto de las unidades de R es el conjunto de los elementos $0 \neq r \in R$, para los cuales $\varphi(r)$ toma valores mínimos.

(42) Sea $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$. Demuestre que

(a) La función $\varphi : R \longrightarrow \mathbb{Z}$ definida por

$$\varphi(a + b\sqrt{2}) = |a^2 - 2b^2|$$

es una función bien definida y además $\varphi(xy) = \varphi(x)\varphi(y)$.

(b) R es un anillo euclidiano con respecto a φ.

(c) Determine las unidades de R.

(d) Si $a + b\sqrt{2} > 1$ es una unidad de R, entonces $a, b \in \mathbb{N}$. En particular entre todas las unidades de R mayores que 1 existe una mínima.

(e) Toda unidad de R tiene la forma $\pm(a+b\sqrt{2})$ con $a, b \in \mathbb{N}_0$ y $a+b\sqrt{2}$ es una unidad de R mayor que 1.

(f) Toda unidad de R tiene la forma $\pm(1 \pm \sqrt{2})^n$ para algún $n \in \mathbb{Z}$.

(43) Sea R un DFU-anillo. Demuestre que si todo ideal de R generado por dos elementos es un ideal principal, entonces R es un anillo de ideales principales.

(44) Presente un ejemplo de un anillo no noetheriano.

(45) Sea K un cuerpo. ¿Se verifica que $K[x]$ es un anillo noetheriano? ¿Es un anillo de ideales principales?

(46) Determine los ideales maximales y los ideales primos del anillo $\mathbb{Z}$.

(47) Demuestre que para $m \in \mathbb{N}$ el polinomio

$$x^{2^m} - 1 \in \mathbb{Q}[x]$$

tiene la siguiente descomposición en factores irreducibles

$$x^{2^m} - 1 = (x-1)(x+1)(x^2+1)(x^4+1)\cdots(x^{2^{m-1}}+1).$$

`Sugerencia:` la existencia de tal descomposición se demuestra por inducción matemática sobre m. La irreducibilidad de los factores demuéstrela con una sustitución adecuada $x \mapsto f \in \mathbb{Q}[x]$ y aplique el criterio de Eisenstein.

(48) Demuestre que el polinomio

$$f = 61x^3 + 5x^2 - 3x + 6$$

es irreducible en $\mathbb{Q}[x]$ y en $\mathbb{Z}[x]$.

(49) Demuestre que el polinomio

$$x^4y^4 - x^3y^2 - 3x^2y^4 + x^4 + x^2y^2 + 2xy^3 + 3y^4 - 17x^3 - xy^2 - xy - 7y + 13$$

es irreducible en $\mathbb{Q}(x)[y]$ y en $\mathbb{Q}(y)[x]$.

(50) Sea K un cuerpo con $\mathrm{Char}(K) = p > 0$ y sea $f = x^p - a \in K[x]$. Demuestre que si a no es una p-potencia en K, entonces f es irreducible sobre K.

(51) Sea K un cuerpo con $\mathrm{Char}(K) = p > 0$ y sea $f = x^p - x - a \in K[x]$. Demuestre que f es irreducible sobre K o f se descompone de la siguiente manera:

$$f = \prod_{j=0}^{p-1}(x - (b + j)),$$

con $b \in K$.

(52) Sea $a \in \mathbb{C}$ una raíz del polinomio $f = x^3 + 3x - 2 \in \mathbb{Q}[x]$.

(a) Demuestre que f es irreducible sobre $\mathbb{Q}$.

(b) Represente los elementos a^{-1}, $(1+a)^{-1} \in \mathbb{Q}(a)$ como combinaciones lineales sobre $\mathbb{Q}$ de $(1, a, a^2)$.

(53) Construya el cuerpo $\mathbb{F}_4$ y descomponga cada $f \in \mathbb{F}_2[x]$ con $\mathrm{grad}(f) \leq 3$ como producto de elementos irreducibles de $\mathbb{F}_4[x]$.

(54) Demuestre que $f = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ es irreducible sobre $\mathbb{Z}_5$.

(55) Sea p un número entero primo. Demuestre que el polinomio

$$f = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$$

es irreducible en $\mathbb{Z}[x]$.

(56) Sea $n \geq 3$. ¿Es $f = x^{2^n} + x + 1 \in \mathbb{Z}_2[x]$ irreducible en $\mathbb{Z}_2[x]$?

(57) Sea p un número primo. Demuestre que el polinomio

$$\Phi_p := \frac{x^p - 1}{x - 1}$$

es irreducible sobre $\mathbb{Q}$.

(58) ¿Existe un polinomio irreducible de grado 4 sobre $\mathbb{Z}_2$? En caso afirmativo, muéstrelo y expréselo en factores lineales sobre alguna extensión de $\mathbb{Z}_2$.

(59) Demuestre que $f = x^3 + 6x^2 + 8x + 4 \in \mathbb{Z}[x]$ es irreducible.

(60) Sea $(G, +)$ un grupo abeliano. Defina sobre G la siguiente multiplicación

$$\forall x \ \forall y \quad xy = 0.$$

Demuestre que $(G, +, \cdot)$ es un anillo conmutativo sin elemento identidad.

(61) Determine el conjunto $U(\mathbb{Z}[\mathrm{i}])$.

(62) Demuestre que el conjunto

$$Q_8 := \{\pm 1, \pm \imath, \pm \jmath, \pm k\}$$

es un grupo no abeliano con la multiplicación definida en el anillo $\mathcal{H}$ de los cuaterniones de Hamilton.

(63) Si n es un natural impar, demuestre que $[2] \in U(\mathbb{Z}_n)$.

(64) Suministre información sobre los divisores de cero del anillo $\mathrm{Mat}(2, \mathbb{R})$.

(65) Sea ζ una raíz cúbica compleja de la unidad. Definamos

$$\mathbb{Z}[\zeta] := \{a + b\zeta \mid a, b \in \mathbb{Z}\}.$$

Demuestre que $\mathbb{Z}[\zeta]$ es un dominio entero y determine $U(\mathbb{Z}[\zeta])$.

(66) Construya un cuerpo con cuatro elementos.

(67) Construya un cuerpo con ocho elementos.

(68) Demuestre que $\mathbb{Z}[x]$ no es un anillo de ideales principales.

(69) Demuestre que $\mathbb{Z}$ es un anillo euclidiano.

(70) Determine los elementos primos de $\mathbb{Z}[\mathrm{i}]$.

(71) `Teorema de Wilson.` Sea p un número primo. Demuestre que

$$(p-1)! \equiv -1 \bmod p.$$

(72) Sea R un anillo conmutativo y $r, s \in R$. Demuestre que

(1) $(r) + (s) = \{rx + sy \mid x, y \in R\}$.
(2) $(r)(s) = (rs)$.

Parte II

Cuerpos

CAPÍTULO 5

EXTENSIONES DE CUERPOS

5.1 Preliminares

Un anillo conmutativo en el cual todo elemento no nulo tiene un inverso se denomina un `cuerpo`. A lo largo de este capítulo, K denota siempre un cuerpo.

5.1.1 Ejemplos. (1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos.

(2) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es un cuerpo.

(3) Si p es un número primo, entonces $\mathbb{Z}_p$ es un cuerpo.

(4) Con $K(x)$ notamos al cuerpo cociente del dominio entero $K[x]$.

5.1.2 Definición. Sea R un anillo. La función $\varphi : \mathbb{Z} \longrightarrow R$ definida por

$$\varphi(n) = n1$$

es un homomorfismo de anillos cuyo núcleo es de la forma $k\mathbb{Z}$ para algún $k \in \mathbb{N}_0$. Este número k coincide con la `característica` de R.

5.1.3 Observación. En términos de la teoría de grupos, observe que $\text{char}(R)$ es el orden del elemento $1 \in R$ en $(R, +)$.

5.1.4 Ejemplos. (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son anillos con característica cero.

(2) $\text{char}(\mathbb{Z}_n) = n$ para todo $n \geq 2$.

(3) $\mathrm{char}(\mathbb{Z}_2(x)) = 2$.

(4) $\mathrm{char}(\mathrm{End}(\mathbb{Z}_3)) = 3$.

5.1.5 Lema. Sea R un anillo y $\mathrm{char}(R) = n \neq 0$. Entonces

(1) $na = 0$ para todo $a \in R$.

(2) Si R no tiene divisores de cero, entonces n es un número primo. En particular, todo cuerpo tiene característica cero o un número primo.

DEMOSTRACIÓN.

(1) Para todo $a \in R$ se verifica que

$$na = n(1a) = (n1)a = 0a = 0.$$

(2) Supongamos que $n = kl$ con $k, l \neq 1$. Entonces

$$0 = n1 = (kl)1 = (k1)(l1).$$

Dado que R no tiene divisores de cero, se verifica que $k1 = 0$ o $l1 = 0$, lo cual contradice la minimalidad de n. □

Es importante tener en cuenta que si un cuerpo es finito, entonces su característica es un número primo. Pero, el hecho que un cuerpo tenga como característica un número primo no garantiza que ese sea finito. Por ejemplo, el cuerpo de las funciones racionales $\mathbb{Z}_2(x)$ tiene característica 2, no obstante es infinito.

5.1.6 Teorema. (El monomorfismo de Frobenius) Sea R un dominio entero con $\mathrm{char}(R) = p \neq 0$. Entonces la función $\varphi : R \longrightarrow R$ definida por

$$\varphi(x) = x^p$$

es un monomorfismo. Si R es finito, entonces φ es un automorfismo, el cual se denomina `automorfismo de Frobenius`.

DEMOSTRACIÓN. Sean $a, b \in R$. Dado que R es conmutativo se tiene que

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b).$$

Por otro lado,

$$\begin{aligned}\varphi(a+b) &= (a+b)^p \\ &= \sum_{j=0}^{p} \binom{p}{j} a^{p-j} b^j \\ &= a^p + \sum_{j=1}^{p-1} \binom{p}{j} a^{p-j} b^j + b^p.\end{aligned}$$

Para todo j con $1 \leq j \leq p-1$ se verifica que $p \mid \binom{p}{j}$. En efecto,

$$\mathbb{Z} \ni \binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!}.$$

Definamos $a := (p-1)\cdots(p-j+1)$. Entonces se tiene que $j! \mid pa$. Dado que $\operatorname{mcd}(p, j!) = 1$, se sigue que $j! \mid a$. En consecuencia,

$$\binom{p}{j} = pm$$

para algún $m \in \mathbb{Z}$ con lo cual se tiene la afirmación. Dado que $\operatorname{char}(R) = p$, se tiene que $\binom{p}{j} = 0$ para todo j con $1 \leq j \leq p-1$. Por lo tanto, $\varphi(a+b) = a^p + b^p$ y se tiene que φ es un homomorfismo.

Dado que R no tiene divisores de cero,

$$a \in \ker(\varphi) \Leftrightarrow a^p = 0 \Leftrightarrow a = 0.$$

En consecuencia, φ es inyectiva, por tanto un monomorfismo. Si R es finito, entonces se tiene la sobreyectividad. □

5.1.7 Definición. (1) Si $L \subseteq K$ es un subanillo de K y L es un cuerpo, entonces decimos que L es un `subcuerpo` de K. Sin dificultades se verifica que la intersección de subcuerpos de L es un subcuerpo de L.

(2) Se define el `cuerpo primo` P de K como la intersección de todos sus subcuerpos. Esto es,

$$P = \bigcap \{U \mid U \text{ es subcuerpo de } K\}.$$

Evidentemente P está contenido en cualquier subcuerpo de K. Es decir, P es el subcuerpo más pequeño de K.

En el siguiente lema demostramos que el tipo de isomorfía del cuerpo primo de un cuerpo K depende exclusivamente de la característica de K.

5.1.8 Lema. Sea P el cuerpo primo de K.

(1) Si $\text{char}(K) = 0$, entonces

$$P = \{(r1)(s1)^{-1} \mid r, s \in \mathbb{Z},\ s \neq 0\} \cong \mathbb{Q}.$$

(2) Si $\text{char}(K) = p$, entonces

$$P = \{n1 \mid n = 0, \ldots, p-1\} \cong \mathbb{Z}_p.$$

DEMOSTRACIÓN. Dado que $1 \in P$, se verifica que $n1 \in P$ para todo $n \in \mathbb{Z}$. La función $\varphi : \mathbb{Z} \longrightarrow P$ definida por

$$\varphi(n) = n1$$

es un homomorfismo de anillos.

(1) Si $\text{char}(K) = 0$, entonces $\ker(\varphi) = \{0\}$. Es decir, φ es un monomorfismo. Aplicando el primer teorema de isomorfía se tiene que

$$\mathbb{Z} \cong \mathbb{Z}/\ker(\varphi) \cong \varphi(\mathbb{Z}) = \{n1 \mid n \in \mathbb{Z}\} \subseteq P.$$

Usando la propiedad universal del cuerpo cociente (teorema 2.3.3), se tiene que existe un único monomorfismo $\Phi : \mathbb{Q} \longrightarrow P$ tal que

$$\mathbb{Q} \cong \Phi(\mathbb{Q}) = \{(r1)(s1)^{-1} \mid r, s \in \mathbb{Z},\ s \neq 0\} \subseteq P.$$

Al ser $\mathbb{Q} \cong \Phi(\mathbb{Q})$ se tiene que $\Phi(\mathbb{Q})$ es un cuerpo. Es decir, $\Phi(\mathbb{Q})$ es un subcuerpo de K y, en consecuencia, se tiene la otra inclusión.

(2) Si $\text{char}(K) = p$, entonces $\ker(\varphi) = p\mathbb{Z}$. Usando nuevamente el primer teorema de isomorfía se tiene que

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker(\varphi) \cong \varphi(\mathbb{Z}) \subseteq P.$$

En consecuencia, $\varphi(\mathbb{Z}) \cong \mathbb{Z}_p$ es un cuerpo. Por lo tanto, $\varphi(\mathbb{Z})$ es un subcuerpo de K y se tiene la otra inclusión. Finalmente, del lema 5.1.5 (1) se sigue que $pa = 0$ para todo $a \in K$. Así se tiene que

$$P = \varphi(\mathbb{Z}) = \{n1 \mid n = 0, \ldots, p-1\}$$

con lo cual se tiene la conclusión. □

5.1.9 Definición. Decimos que un cuerpo L es una `extensión` de K si existe un monomorfismo $i : K \longrightarrow L$. Usaremos la notación L/K. Es claro que

$$K \cong i(K) \leq L,$$

por lo tanto, es usual identificar K con $i(K)$ y escribir $K \subseteq L$.

5.1.10 Ejemplos. Son extensiones de cuerpos: $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ y $K(x)/K$.

5.1.11 Observación. Si L/K es una extensión de cuerpos, entonces podemos dotar a L de una estructura de espacio vectorial sobre K. En efecto, $(L,+)$ es un grupo abeliano y podemos definir una multiplicación por escalar

$$\cdot : K \times L \longrightarrow L$$

de la siguiente manera:

$$(k,l) \longmapsto kl$$

para todo $k \in K$ y $l \in L$.

5.1.12 Definición. Sea L/K una extensión de cuerpos. La dimensión de L sobre K se nota con $|L:K|$ y se denomina `el grado` de la extensión. Si $|L:K| \in \mathbb{N}$, entonces decimos que la extensión L/K es `finita`. En caso contrario decimos que la extensión es `infinita`. Las extensiones de grado 2 se denominan `cuadráticas`, y las de grado 3 se denominan `cúbicas`.

5.1.13 Ejemplos. Sean K y L cuerpos.

(1) $|L:K| = 1$ si y solo si $K = L$. Note que $B = (1)$ es una base para L sobre K.

(2) $|\mathbb{C}:\mathbb{R}| = 2$, ya que $B = (1, \mathrm{i})$ es una base para $\mathbb{C}$ sobre $\mathbb{R}$.

(3) $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2$, ya que $B = (1, \sqrt{2})$ es una base para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

(4) $K(x)/K$ no es una extensión finita ya que $B = \{x^j \mid j \in \mathbb{N}_0\}$ es un conjunto linealmente independiente sobre K.

(5) $\mathbb{R}/\mathbb{Q}$ no es una extensión finita. Se puede demostrar que toda extensión finita de $\mathbb{Q}$ es infinita enumerable.

5.1.14 Definición. Sea L/K una extensión de cuerpos. Si M es un cuerpo y $K \subseteq M \subseteq L$, entonces decimos que M es un `cuerpo intermedio` de la extensión L/K.

5.1.15 Ejemplos. (1) $\mathbb{R}$ es cuerpo intermedio de $\mathbb{C}/\mathbb{Q}$.

(2) $\mathbb{Q}(\sqrt{2})$ es cuerpo intermedio de $\mathbb{R}/\mathbb{Q}$.

(3) Si en la propiedad universal (teorema A.2.1) tomamos $S = K[x]$ y definimos Φ mediante $\Phi(x) = x^n$ con $n \in \mathbb{N}$, entonces $\mathrm{Im}(\Phi)$ es el dominio entero dado por

$$\Phi(K[x]) = K[x^n] \subseteq K[x].$$

El cuerpo cociente $K(x^n) := Q(K[x^n])$ satisface

$$K \subseteq K(x^n) \subseteq K(x).$$

Es decir, $K(x^n)$ es un cuerpo intermedio de $K(x)/K$.

5.1.16 Teorema. (Fórmula del grado) Sea M un cuerpo intermedio de la extensión L/K. Entonces

$$|L : K| = |L : M|\ |M : K|.$$

Demostración. Sean $B_1 = (v_i \mid i \in I)$ una base para L sobre M y $B_2 = (w_j \mid j \in J)$ una base para M sobre K. Demostramos que

$$B := (w_j v_i \mid j \in J,\ i \in I)$$

es una base para L sobre K. Recordemos que todas las sumas que aparezcan tienen solo un número finito de términos no nulos.

Sea $a \in L$. Entonces

$$a = \sum_{i \in I} a_i v_i, \quad \text{con } a_i \in M,$$

además cada $a_i \in M$ tiene la forma

$$a_i = \sum_{j \in J} k_{ij} w_j, \quad \text{con } k_{ij} \in K.$$

Por lo tanto,

$$a = \sum_{i \in I} \sum_{j \in J} k_{ij} w_j v_i.$$

Esto demuestra que B es un sistema de generadores de L sobre K.

Supongamos ahora que

$$\sum_{i \in I} \Big(\sum_{j \in J} k_{ij} w_j \Big) v_i = 0.$$

Entonces, dado que B_1 es una base para todo $i \in I$ se verifica que

$$\sum_{j \in J} k_{ij} w_j = 0.$$

Dado que B_2 es una base, se tiene entonces que $k_{ij} = 0$ para todo $i \in I$ y para todo $j \in J$. Esto demuestra la independencia lineal de B. □

5.1.17 Corolario. Sea M un cuerpo intermedio de una extensión finita L/K. Entonces

(1) $|L : M|$ y $|M : K|$ son divisores de $|L : K|$.

(2) Si $|L : M| = |L : K|$, entonces $K = M$.

(3) Si $|L : K|$ es un número primo, entonces $M = L$ o $M = K$.

(4) Sean $K = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_{r-1} \subseteq M_r = L$ cuerpos intermedios de L/K. Entonces

$$|L : K| = \prod_{j=1}^{r} |M_j : M_{j-1}|.$$

DEMOSTRACIÓN. (1) Es consecuencia inmediata del teorema de la fórmula del grado.

(2) De la fórmula del grado se sigue que $|M : K| = 1$. Sea $B = (m)$ una base para M sobre K. Se verifica que existe $k \in K$ tal que $1 = mk$. Es decir, $m^{-1} \in K$. Sea ahora $x \in M$ cualquiera. Entonces $x = tm$ para algún $t \in K$. Por lo tanto, $m^{-1}x \in K$ y se sigue que $x \in K$. Esto demuestra que $M \subseteq K$. La otra inclusión es clara.

(3) Se sigue de (2).

(4) Usamos inducción matemática sobre r. Si $r = 1$, entonces la afirmación se verifica inmediatamente.

Supongamos que

$$|M_{r-1} : K| = \prod_{j=1}^{r-1} |M_j : M_{j-1}|.$$

Entonces

$$|L : K| = |L : M_{r-1}|\ |M_{r-1} : K| = \prod_{j=1}^{r} |M_j : M_{j-1}|,$$

con lo cual se tiene la conclusión. □

5.1.18 Observaciones. (1) Una consecuencia del corolario anterior es que no existen cuerpos intermedios entre $\mathbb{C}$ y $\mathbb{R}$.

(2) A pesar de que $\mathbb{C} \neq \mathbb{R}$ se verifica que

$$|\mathbb{C} : \mathbb{Q}| = |\mathbb{C} : \mathbb{R}||\mathbb{R} : \mathbb{Q}| = |\mathbb{R} : \mathbb{Q}|.$$

Supongamos ahora que se tiene una extensión de cuerpos L/K y un subconjunto A de L. Presentamos a continuación una técnica para construir el cuerpo intermedio más pequeño de L/K, que contiene a A.

5.1.19 Definición. Sean L/K una extensión de cuerpos, $A \subseteq L$ y

$$\mathcal{R} := \{R \mid R \text{ es subanillo de } L \text{ y } K \cup A \subseteq R\} \tag{5.1}$$

$$\mathcal{M} := \{M \mid M \text{ es subcuerpo de } L \text{ y } K \cup A \subseteq M\}. \tag{5.2}$$

(1) Notamos con $K[A]$ al subanillo más pequeño de L que contiene a $K \cup A$. Esto es,

$$K[A] = \bigcap \mathcal{R}.$$

$K[A]$ se llama el subanillo de L `generado por` A `sobre` K.

(2) Notamos con $K(A)$ al subcuerpo más pequeño de L que contiene a $K \cup A$. Esto es,

$$K(A) = \bigcap \mathcal{M}.$$

$K(A)$ se llama el subcuerpo de L `generado por` A `sobre` K o también el subcuerpo de L formado a partir de K `por adjunción de` A.

(3) La extensión L/K se denomina `finitamente generada` si existe un conjunto finito $A \subseteq L$ tal que $L = K(A)$. Si $A = \{a_1, \ldots, a_n\}$, entonces escribiremos $L = K(a_1, \ldots, a_n)$, en lugar de $L = K(\{a_1, \ldots, a_n\})$.

(4) Si $A = \{a\}$ y $L = K(a)$, entonces decimos que L/K es una extensión `simple`. En este caso, decimos que a es un elemento `primitivo` de la extensión.

5.1.20 Ejemplos. (1) La extensión $\mathbb{C}/\mathbb{R}$ es simple, ya que $\mathbb{C} = \mathbb{R}[z] = \mathbb{R}(z)$ para todo $z \in \mathbb{C} \setminus \mathbb{R}$. Por lo tanto, todo número complejo, no real, es un elemento primitivo.

(2) La extensión $K(x)/K$ es simple y x es un elemento primitivo.

(3) La extensión $\mathbb{R}/\mathbb{Q}$ no es simple.

(4) Si $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$, entonces $L/\mathbb{Q}$ es simple. En efecto, definamos $a := \sqrt{2} + \sqrt{3}$ y demostremos que $L = \mathbb{Q}(a)$. Es claro que $\mathbb{Q}(a) \subseteq L$.

Recíprocamente, note que

$$a^2 = 5 + 2\sqrt{6} \in \mathbb{Q}(a).$$

Por lo tanto, $\sqrt{6} \in \mathbb{Q}(a)$. Note además que

$$\sqrt{2} = a\sqrt{6} - 2a \in \mathbb{Q}(a)$$
$$\sqrt{3} = a\sqrt{6} - 3a \in \mathbb{Q}(a).$$

En consecuencia, $\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\} \subseteq \mathbb{Q}(a)$ y se tiene que $L \subseteq \mathbb{Q}(a)$.

5.1.21 Lema. Sean L/K una extensión de cuerpos y $A, B \subseteq L$. Entonces

(1) $K[A] \subseteq K(A)$.

(2) Si $A \subseteq B$, entonces $K(A) \subseteq K(B)$.

(3) $K(A \cup B) = K(A)(B)$.

Demostración.

(1) Se sigue del hecho que $\mathcal{M} \subseteq \mathcal{R}$.

(2) Si $A \subseteq B$, entonces $K \cup A \subseteq K \cup B \subseteq K(B)$. Por lo tanto

$$K(A) \subseteq K(B).$$

(3) Note inicialmente que

$$K \cup (A \cup B) = (K \cup A) \cup B \subseteq K(A) \cup B \subseteq K(A)(B).$$

Por lo tanto, $K(A \cup B) \subseteq K(A)(B)$.

Recíprocamente, de (2) se sigue que $K(A) \cup B \subseteq K(A \cup B)$ y, en consecuencia,

$$K(A)(B) \subseteq K(A \cup B),$$

con lo cual se completa la prueba. □

En el siguiente lema presentamos una caracterización de los elementos de $K[A]$ y $K(A)$.

5.1.22 Lema. Sean L/K una extensión de cuerpos, $c, a_1, \ldots, a_n \in L$ y $A \subseteq L$. Entonces

(1) $K(A) = \{ab^{-1} \mid a, b \in K[A],\ b \neq 0\} \cong Q(K[A])$.

(2) $K[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in K[x_1, \ldots, x_n]\}$.

En particular se verifica que

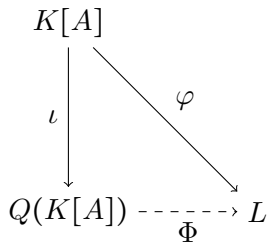
$$K[c] = \{f(c) \mid f \in K[x]\}.$$

Demostración.

(1) Definamos

$$F := \{ab^{-1} \mid a, b \in K[A],\ b \neq 0\}.$$

La isomorfía entre F y el cuerpo cociente $Q(K[A])$ es una consecuencia inmediata de la propiedad universal del cuerpo cociente.



En efecto, es suficiente tomar φ como la función idéntica en el teorema 2.3.3 y se tiene que

$$\begin{aligned}\Phi(Q(K[A])) &= \{\Phi(\tfrac{a}{b}) \mid a, b \in K[A],\ b \neq 0\}\\ &= \{\varphi(a)\varphi(b)^{-1} \mid a, b \in K[A],\ b \neq 0\}\\ &= \{ab^{-1} \mid a, b \in K[A],\ b \neq 0\}\\ &= F.\end{aligned}$$

Dado que Φ es un monomorfismo se tiene que

$$F = \Phi(Q(K[A])) \cong Q(K[A]).$$

Por lo tanto, F es un cuerpo y además contiene a $K \cup A$. En consecuencia, $K(A) \subseteq F$. Recíprocamente, dado que $K[A] \subseteq K(A)$, se verifica que $F \subseteq K(A)$.

(2) Sea $\Phi : K[x_1, \ldots, x_n] \longrightarrow L$ el homomorfismo de sustitución del teorema A.3.2 y definamos $F := \Phi(K[x_1, \ldots, x_n])$. Esto es,

$$F = \{f(a_1, \ldots, a_n) \mid f \in K[x_1, \ldots, x_n]\}.$$

Dado que F es la imagen homomórfica de un anillo, se sigue que F es un subanillo de L. Por otro lado, es claro que F contiene todos los elementos $a_1, \ldots, a_n$ con lo cual se tiene que $K[a_1, \ldots, a_n] \subseteq F$. La otra contenencia es inmediata. □

5.2 Extensiones algebraicas

5.2.1 Definición. Sea L/K una extensión de cuerpos y $a \in L$.

(1) Decimos que a es `algebraico` sobre K si existe $0 \neq f \in K[x]$ tal que $f(a) = 0$. En caso contrario, es decir, si para todo $0 \neq f \in K[x]$ se verifica que $f(a) \neq 0$, entonces decimos que a es `trascendente` sobre K.

(2) La extensión L/K se denomina `algebraica` si todo elemento de L es algebraico sobre K. En caso contrario, esta se denomina trascendente.

5.2.2 Ejemplos. (1) Todo $a \in K$ es algebraico sobre K, ya que este es raíz de $f = x - a \in K[x]$.

(2) La indeterminada $x \in K(x)$ es trascendente sobre K. En efecto para todo $f \in K[x]$ se verifica que $f(x) = f$. Por lo tanto, $f(x) = 0$ si y solo si $f = 0$.

(3) La extensión $\mathbb{C}/\mathbb{R}$ es algebraica, ya que para todo $z = a + bi \in \mathbb{C}$ se verifica que z es raíz del polinomio

$$f = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x].$$

(4) $\sqrt[3]{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, ya que para $f = x^3 - 2 \in \mathbb{Q}[x]$ se cumple que $f(\sqrt[3]{2}) = 0$.

(5) Charles Hermite demostró, en 1873, que e es trascendente sobre $\mathbb{Q}$.

(6) Ferdinand von Lindemann demostró, en 1882, que π es trascendente sobre $\mathbb{Q}$.

5.2.3 Teorema. Sean L/K una extensión de cuerpos y $a \in L$ algebraico sobre K. Entonces

(1) Existe un único polinomio mónico $m_{a,K} \in K[x]$ irreducible sobre K que satisface $m_{a,K}(a) = 0$.

(2) Si $f \in K[x]$ satisface $f(a) = 0$, entonces $m_{a,K} \mid f$.

(3) Si $f \in K[x]$ es mónico, irreducible y satisface $f(a) = 0$, entonces $f = m_{a,K}$.

(4) a es algebraico sobre todo cuerpo intermedio M de L/K y, además, $m_{a,M} \mid m_{a,K}$ en $M[x]$.

Demostración.

(1) `Existencia.` Sea $\varphi : K[x] \longrightarrow L$ la función sustitución en a. Entonces

$$\ker(\varphi) = \{f \in K[x] \mid f(a) = 0\}.$$

Dado que a es algebraico sobre K, se tiene que $\ker(\varphi) \neq \varnothing$. Dado que $\ker(\varphi)$ es un ideal de $K[x]$, del primer teorema de isomorfía se sigue que

$$K[x]/\ker(\varphi) \cong \mathrm{Im}(\varphi) \subseteq L.$$

Es claro que $\mathrm{Im}(\varphi)$ no tiene divisores de cero. Por lo tanto, del teorema 3.1.8 se sigue que $\ker(\varphi)$ es un ideal primo.

Por otro lado, dado que $K[x]$ es un anillo de ideales principales, se verifica que $\ker(\varphi)$ es un ideal principal generado por un elemento primo y, por lo tanto, irreducible. Esto es: $\ker(\varphi) = (g)$. Si b_n es el coeficiente principal de g, entonces definimos

$$m_{a,K} = \tfrac{1}{b_n} g.$$

Se verifica inmediatamente que $m_{a,K}$ es mónico, irreducible sobre K, que

$$\ker(\varphi) = (g) = (m_{a,K})$$

y, además, $m_{a,K}(a) = 0$.

`Unicidad.` Se sigue del hecho que $m_{a,K}$ es mónico.

(2) Si $f(a) = 0$, entonces $f \in (m_{a,K})$. En consecuencia, $m_{a,K} \mid f$.

(3) De (2) se sigue que $m_{a,K} \mid f$. Por lo tanto, existe $g \in K[x]$ tal que $f = m_{a,K} \cdot g$. De la irreducibilidad de f se sigue que $g \in K$. Finalmente, dado que f es mónico, se sigue que $g = 1$.

(4) Note que $m_{a,K} \in M[x]$ y $m_{a,K}(a) = 0$. Por lo tanto, de (2) se sigue que $m_{a,M} \mid m_{a,K}$ en $M[x]$. □

5.2.4 Definición. Sean L/K una extensión de cuerpos y $a \in L$ algebraico sobre K. El polinomio $m_{a,K} \in K[x]$ garantizado por el teorema anterior se denomina el `polinomio minimal` de a sobre K. Si en el contexto no hay lugar a confusión, escribimos m_a en lugar de $m_{a,K}$.

5.2.5 Ejemplos. (1) Para todo $a \in K$ se verifica que $m_{a,K} = x - a$.

(2) Sea $a = \mathrm{i} \in \mathbb{C}$. Entonces $m_{a,\mathbb{Q}} \in \mathbb{Q}[x]$ está dado por $m_{a,\mathbb{Q}} = x^2 + 1$.

(3) Sea $a = \sqrt{2} \in \mathbb{R}$. Entonces $m_{a,\mathbb{Q}} \in \mathbb{Q}[x]$ está dado por $m_{a,\mathbb{Q}} = x^2 - 2$.

(4) Sea $a = \sqrt[3]{2} \in \mathbb{R}$. Entonces $m_{a,\mathbb{Q}} = x^3 - 2 \in \mathbb{Q}[x]$.

(5) Sea $a = \sqrt{2} + \sqrt{3} \in \mathbb{R}$. Entonces $m_{a,\mathbb{Q}} = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$.

(6) Sea $a = \frac{1}{\sqrt{2}}(1 - \mathrm{i})$. Entonces $m_{a,\mathbb{Q}} = x^4 + 1$. Note que

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$$

sobre $\mathbb{Q}(\sqrt{2})$ y sobre $\mathbb{R}$. Entonces

$$m_{a,\mathbb{Q}(\sqrt{2})} = m_{a,\mathbb{R}} = x^2 - \sqrt{2}x + 1 \mid m_{a,\mathbb{Q}}.$$

En el siguiente teorema examinamos la estructura de la extensión simple $K(a)/K$ con a un elemento de una extensión de K. En este proceso juega un papel importante el anillo de los polinomios $K[x]$. Demostramos que si a es algebraico sobre K, entonces $K(a) \cong K[x]/(m_a)$ y si a es trascendente sobre K, entonces $K(a) \cong K(x)$.

5.2.6 Teorema. Sean L/K una extensión de cuerpos y $a \in L$.

(1) Si a es algebraico sobre K, entonces $K(a) = K[a] \cong K[x]/(m_a)$

(2) Si a es algebraico sobre K y $n = \text{grad}(m_a)$, entonces

$$B = (1, a, \ldots, a^{n-1})$$

es una base para $K(a)$ sobre K. En particular

$$|K(a) : K| = \text{grad}(m_a).$$

(3) Si a es trascendente sobre K, entonces $K(a) \cong K(x)$ y

$$|K(a) : K| \notin \mathbb{N}.$$

Demostración.

(1) Sea $\varphi : K[x] \longrightarrow K[a]$ el homomorfismo de sustitución. Del lema 5.1.22 (2) se sigue que φ es sobreyectiva. Además

$$\ker(\varphi) = \{f \mid f \in K[x],\ f(a) = 0\} = (m_a).$$

Usando el primer teorema de isomorfía se tiene que

$$K[x]/(m_a) = K[x]/\ker(\varphi) \cong \text{Im}(\varphi) = K[a].$$

Dado que m_a es irreducible y $K[x]$ es un anillo de ideales principales, se verifica que (m_a) es un ideal maximal de $K[x]$ y, por lo tanto, $K[x]/(m_a)$ es un cuerpo. En consecuencia, $K[a]$ es un cuerpo y se tiene la igualdad.

(2) Sea φ nuevamente el homomorfismo de sustitución. Entonces de la sobreyectividad se sigue que dado $b \in K(a)$ existe $g \in K[x]$ tal que $b = g(a)$. Aplicando el algoritmo de Euclides tenemos que

$$g = m_a q + r, \quad \text{con } \text{grad}(r) < \text{grad}(m_a).$$

Entonces

$$r(a) = g(a) - m_a(a)q(a) = g(a) = b.$$

Esto demuestra que dado $b \in K(a)$ siempre es posible encontrar $g \in K[x]$ con $\text{grad}(g) < \text{grad}(m_a)$ y $g(a) = b$.

Entonces si $g = \sum_{j=0}^{n-1} k_j x^j$, se verifica que

$$b = g(a) = \sum_{j=0}^{n-1} k_j a^j.$$

Por lo tanto, $B = (1, a, \ldots, a^{n-1})$ es un sistema de generadores para $K(a)$ sobre K.

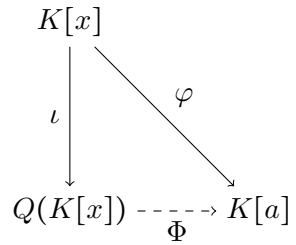
Para demostrar la independencia lineal de B, supongamos que $\sum_{j=0}^{n-1} k_j a^j = 0$ con $k_j \in K$ y no todos estos son cero. Si definimos

$$h := \sum_{j=0}^{n-1} k_j x^j,$$

entonces $h(a) = 0$ y se tendría que $m_a \mid h$, lo cual es una contradicción, ya que

$$\text{grad}(m_a) = n > n - 1 \geq \text{grad}(h).$$

(3) Sea $\varphi : K[x] \longrightarrow K[a]$ el homomorfismo de sustitución. Entonces de la trascendencia de a se sigue que $\ker(\varphi) = \{0\}$ y se tiene que φ es un monomorfismo. Del lema 5.1.22 (2) se infiere que φ es sobre y, por lo tanto, un isomorfismo.



De la propiedad universal del cuerpo cociente (teorema 2.3.3) se sigue que la función

$$\Phi : K(x) \longrightarrow K[a]$$

es un isomorfismo. En consecuencia,

$$K(x) \cong K[a].$$

Es decir, $K[a]$ es un cuerpo. Además $K \cup \{a\} \subseteq K[a]$, por lo tanto $K(a) \subseteq K[a]$. La otra inclusión se tiene siempre.

De la trascendencia de a se sigue que el conjunto $\{1, a, a^2, \ldots\}$ es linealmente independiente sobre K. Por lo tanto, $|K(a) : K| \notin \mathbb{N}$. $\square$

5.2.7 Observación. Como consecuencia del teorema anterior, si $\text{grad}(m_a) = n$, entonces

$$K(a) = \Big\{ \sum_{j=0}^{n-1} k_j a^j \mid k_j \in K \Big\}. \tag{5.3}$$

5.2.8 Ejemplos. (1) Dado que $m_{\mathrm{i},\mathbb{R}} = x^2 + 1$, se tiene que $|\mathbb{C} : \mathbb{R}| = 2$. Por lo tanto, del teorema anterior se verifica que

$$\begin{aligned} \mathbb{R}(\mathrm{i}) &= \{g(\mathrm{i}) \mid g \in \mathbb{R}[x],\ \text{grad}(g) < 2\} \\ &= \{a + b\mathrm{i} \mid a, b \in \mathbb{R}\} \\ &= \mathbb{C}. \end{aligned}$$

(2) Sea la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Sabemos que $m_{\sqrt{2}} = x^2 - 2$. Por lo tanto, $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$ y así

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

(3) Sea la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Sabemos que $m_{\sqrt[3]{2}} = x^3 - 2$. Por consiguiente, $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ y así

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

El hecho que una extensión de cuerpos L/K sea algebraica tiene múltiples consecuencias. En lo que sigue abordaremos algunas caracterizaciones de estas.

5.2.9 Teorema. Sea L/K una extensión de cuerpos. Las siguientes afirmaciones son equivalentes:

(1) L/K es una extensión finita.

(2) L/K es una extensión algebraica y finitamente generada.

(3) Existen $a_1, \ldots, a_n \in L$ algebraicos sobre K tales que

$$L = K(a_1, \ldots, a_n).$$

Demostración.

(1) $\Rightarrow$ (2). Sea $n := |L : K| \in \mathbb{N}$. Entonces para todo $b \in L$ se verifica que el conjunto $\{1, b, \ldots, b^n\}$ es linealmente dependiente sobre K. Por lo tanto, existen $k_0, \ldots, k_n \in K$ no todos nulos, tales que

$$\sum_{j=0}^{n} k_j b^j = 0.$$

Si definimos $f = \sum_{j=0}^{n} k_j x^j$, se tiene que $0 \neq f \in K[x]$ y $f(b) = 0$. Esto demuestra que b es algebraico sobre K.

Sea $B = (a_1, \ldots, a_n)$ una base para L sobre K. Es inmediato que $K(a_1, \ldots, a_n) \subseteq L$.

Recíprocamente, si $l \in L$, entonces $l = \sum_{j=1}^{n} k_j a_j \in K(a_1, \ldots, a_n)$ y se tiene que

$$L = K(a_1, \ldots, a_n).$$

(2) $\Rightarrow$ (3). Evidente.

(3) $\Rightarrow$ (1). Demostramos por inducción matemática sobre n que

$$|K(a_1, \ldots, a_n) : K| \in \mathbb{N}.$$

Si $n = 1$, entonces el resultado se sigue del teorema 5.2.6 (2).

Supongamos que la afirmación es válida para $n - 1$.

Definamos $M := K(a_1, \ldots, a_{n-1})$. Del lema 5.1.21 se sigue que $L = M(a_n)$. Dado que a_n es algebraico sobre K, también lo es sobre M. Por lo tanto, con la fórmula del grado tenemos que

$$|L : K| = |M(a_n) : K| = \underbrace{|M(a_n) : M|}_{\in \mathbb{N}} \underbrace{|M : K|}_{\in \mathbb{N}} \in \mathbb{N}.$$

□

5.2.10 Observación. En el teorema anterior se demostró que toda extensión finita es algebraica. Sin embargo, mostramos más adelante que existen extensiones algebraicas infinitas.

Demostramos a continuación que la propiedad `ser extensión algebraica` es transitiva.

5.2.11 Teorema. Sea M un cuerpo intermedio de la extensión L/K con M/K algebraica.

(1) Si $a \in L$ es algebraico sobre M, entonces a es algebraico sobre K.

(2) Si L/M es algebraica, entonces L/K es algebraica.

Demostración.

(1) Si $a \in L$ es algebraico sobre M, entonces existe $f = \sum_{j=0}^{n} b_j x^j \in M[x]$ tal que $f(a) = 0$. Es decir, existen $b_0, \ldots, b_{n-1} \in M$ tales que

$$a^n + b_{n-1} a^{n-1} + \ldots + b_0 = 0.$$

Si definimos $\widehat{K} := K(b_0, \ldots, b_{n-1})$, entonces lo anterior demuestra que a es algebraico sobre $\widehat{K}$.

Dado que M/K es algebraica, se tiene que cada $b_j \in M$ es algebraico sobre K. Con la fórmula del grado tenemos:

$$|K(a) : K| \leq |\widehat{K}(a) : K| = \underbrace{|\widehat{K}(a) : \widehat{K}|}_{\in \mathbb{N}} \ \underbrace{|\widehat{K} : K|}_{\in \mathbb{N}}.$$

Entonces la extensión $K(a)/K$ es finita y, en consecuencia, a es algebraico sobre K.

(2) Se sigue inmediatamente de (1). □

En el siguiente lema se demuestra que los anillos intermedios de una extensión algebraica son cuerpos.

5.2.12 Lema. Sea L/K un extensión de cuerpos, algebraica y sea R un anillo con $K \subseteq R \subseteq L$. Entonces R es un cuerpo. En particular para todo $A \subseteq L$ se verifica que $K[A] = K(A)$.

Demostración. Es suficiente demostrar que todo elemento no nulo de R tiene un inverso en R. Sea $0 \neq a \in R$. Dado que a es algebraico sobre K, del teorema 5.2.6 se sigue que $K[a] = K(a)$. Por lo tanto, $a^{-1} \in K[a] \subseteq R$. □

5.2.13 Lema. Sean L/K una extensión de cuerpos y $A \subseteq L$. Defina

$$\mathcal{V}_A := \{V \mid V \subseteq A,\ |V| < \infty\}.$$

Entonces

$$K[A] = \bigcup\{K[V] \mid V \in \mathcal{V}_A\}$$

y

$$K(A) = \bigcup\{K(V) \mid V \in \mathcal{V}_A\}.$$

Demostración. Definamos $R := \bigcup\{K[V] \mid V \in \mathcal{V}_A\}$ y $S := \bigcup\{K(V) \mid V \in \mathcal{V}_A\}$. Si $r \in R$, entonces existe $V \in \mathcal{V}_A$ tal que $r \in K[V]$. Por lo tanto, $r \in K[A]$. Es decir, $R \subseteq K[A]$. Similar se demuestra que $S \subseteq K(A)$.

Sean $r_1, r_2 \in R$. Entonces existen $V_1, V_2 \in \mathcal{V}_A$ tales que $r_1 \in K[V_1]$ y $r_2 \in K[V_2]$. Por lo tanto, $r_1, r_2 \in K[V_1 \cup V_2]$ y, consecuentemente:

$$r_1 + r_2,\ r_1 - r_2,\ r_1 r_2 \in K[V_1 \cup V_2] \subseteq R.$$

Con esto se tiene que R es un anillo que contiene a $K \cup A$. Entonces, $K[A] \subseteq R$. Con un argumento similar se demuestra que $K(A) \subseteq S$. □

5.2.14 Teorema. Sean L/K una extensión de cuerpos y $B \subseteq L$.

(1) Si todo elemento de B es algebraico sobre K, entonces $K[B] = K(B)$ y la extensión $K(B)/K$ es algebraica.

(2) Sea $\mathrm{Alg}(L/K) := \{l \in L \mid l \text{ es algebraico sobre } K\}$. Entonces $\mathrm{Alg}(L/K)$ es un subcuerpo de L.

Demostración.

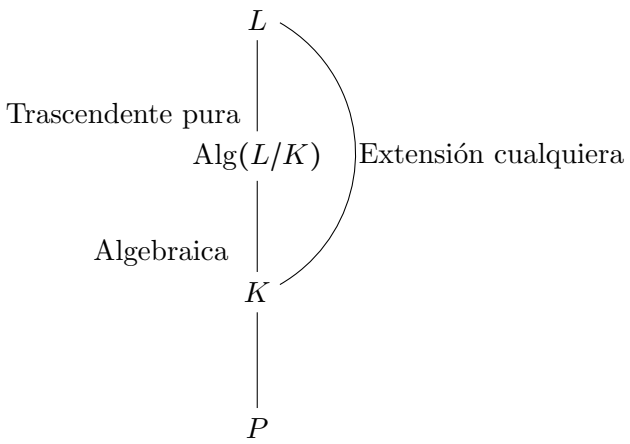
(1) Sean $\mathcal{V}_B := \{V \mid V \subseteq B,\ |V| < \infty\}$ y $V \in \mathcal{V}_B$. Del teorema 5.2.9 se sigue que $K(V)/K$ es una extensión finitamente generada y algebraica. Del lema 5.2.12 se tiene que $K(V) = K[V]$ y del lema 5.2.13 se tiene que

$$\begin{aligned} K(B) &= \bigcup\{K(V) \mid V \in \mathcal{V}_B\} \\ &= \bigcup\{K[V] \mid V \in \mathcal{V}_B\} \\ &= K[B]. \end{aligned}$$

Sea $a \in K(B)$. Entonces $a \in K(V)$ para algún $V \in \mathcal{V}_B$. Dado que $K(V)/K$ es una extensión algebraica, se tiene que a es algebraico sobre K. Por lo tanto, $K(B)/K$ es algebraica.

(2) Definamos $A := \mathrm{Alg}(L/K)$. Claramente $A \subseteq K(A)$. De (1) se sigue que la extensión $K(A)/K$ es algebraica. Por lo tanto, $K(A) \subseteq A$ y consecuentemente $A = K(A)$, el cual es un subcuerpo de L. □

Del teorema anterior se sigue que todo $b \in L \setminus A$ es trascendente sobre A. Una extensión de cuerpos L/K con la propiedad que todo $b \in L \setminus K$ es trascendente sobre K se denomina `trascendente pura`.



5.2.15 Ejemplo. Sea $A := \mathrm{Alg}(\mathbb{C}/\mathbb{Q})$. Del teorema anterior se sigue que A es un subcuerpo de $\mathbb{C}$ y, además, $A/\mathbb{Q}$ es una extensión algebraica. Demostramos que $|A : \mathbb{Q}| \notin \mathbb{N}$.

Supongamos que $|A : \mathbb{Q}| = n$ para algún $n \in \mathbb{N}$. Sea $f = x^p + p$ con p un número primo. Usando el criterio de Eisenstein se sigue que f es irreducible sobre $\mathbb{Q}$. Es conocido que f tiene una raíz en $\mathbb{C}$, digamos a. Por lo tanto, del teorema 5.2.3 (3) se sigue que $f = m_{a,\mathbb{Q}}$ y, en consecuencia,

$$|\mathbb{Q}(a) : \mathbb{Q}| = \mathrm{grad}(m_{a,\mathbb{Q}}) = p.$$

Dado que a es algebraico sobre $\mathbb{Q}$, se verifica que

$$\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq A.$$

Aplicando la fórmula del grado se tiene que

$$n = |A : \mathbb{Q}| = |A : \mathbb{Q}(a)|\ |\mathbb{Q}(a) : \mathbb{Q}| = p\ |A : \mathbb{Q}(a)|.$$

Esto demuestra que todo número primo p divide a n, lo cual no es posible.

5.2.16 Lema. Sea L/K una extensión de cuerpos algebraica. Entonces

(1) Si K es infinito, entonces $|L| = |K|$.

(2) Si K es finito, entonces $|L| \leq |\mathbb{N}|$.

Demostración. Sea $\mathcal{M}$ el conjunto de todos los polinomios mónicos irreducibles con coeficientes en K. Para $f \in \mathcal{M}$ definamos

$$N(f) := \{a \in L \mid f(a) = 0\} \subseteq L.$$

Claramente $N(f)$ es un conjunto finito. Se sigue inmediatamente que

$$\bigcup\{N(f) \mid f \in \mathcal{M}\} \subseteq L.$$

Recíprocamente, sea $a \in L$. Entonces tomando $f = x - a$ se verifica que $f(a) = 0$ y, en consecuencia, $a \in N(f)$. Por lo tanto,

$$L = \bigcup\{N(f) \mid f \in \mathcal{M}\}.$$

(1) Si K es infinito, entonces dado que $|\mathcal{M}| = |K|$, se verifica que

$$|L| \leq |\mathbb{N}| \cdot |K| = |K|.$$

En consecuencia, $|L| = |K|$.

(2) Si K es finito, entonces $|\mathcal{M}| \leq |\mathbb{N}|$. Por lo tanto, $|L| \leq |\mathbb{N}| \cdot |\mathbb{N}| = |\mathbb{N}|$. □

Dado que $\mathbb{Q}$ es enumerable y $\mathbb{R}$ es infinito no enumerable, como consecuencia del lema anterior se tiene el siguiente resultado.

5.2.17 Corolario. (George Cantor) Existe un número infinito no enumerable de números reales trascendentes sobre $\mathbb{Q}$.

5.3 La clausura algebraica

Es conocido que el polinomio $f = x^2 + 1 \in \mathbb{R}[x]$ no puede descomponerse en factores lineales sobre $\mathbb{R}$. Sin embargo, si es posible hacer tal factorización sobre $\mathbb{C}$. Más aún, el teorema fundamental del álgebra establece que todo polinomio no constante $f \in \mathbb{C}[x]$ tiene una raíz en $\mathbb{C}$. Por lo tanto, f puede descomponerse en $\mathbb{C}$ en factores lineales. Una pregunta interesante entonces es: dado un cuerpo K y un polinomio $f \in K[x]$, ¿puede encontrarse una extensión L de K en la cual f tenga todas sus raíces? En esta sección nos ocupamos de dar respuesta a este interrogante.

Sea $f \in K[x]$. En lo que sigue notamos con (f) el ideal de $K[x]$ generado por f. Es decir, $(f) = fK[x]$.

5.3.1 Teorema. (Leopold Kronecker, 1882) Sea $f \in K[x]$ irreducible. Entonces

(1) El anillo $L := K[x]/(f)$ es un cuerpo.

(2) La función $\pi : K \longrightarrow L$ definida por $\pi(a) = a + (f)$ es inyectiva. Es decir, podemos identificar K con $\pi(K)$ y ver a L como una extensión de K.

(3) El polinomio $f \in K[x] \subseteq L[x]$ tiene una raíz en L. Esta raíz está dada por $a := x + (f)$.

(4) $|L : K| = \text{grad}(f)$.

Demostración.

(1) Del lema 4.1.14 se sigue que (f) es un ideal maximal de $K[x]$. Por lo tanto, del teorema 3.1.3 se sigue que L es un cuerpo.

(2) Es claro que π es un homomorfismo. Para demostrar la inyectividad, sean $a, b \in K$. Entonces
$$\pi(a) = \pi(b) \Leftrightarrow a + (f) = b + (f) \Leftrightarrow a - b \in (f).$$
Dado que $\text{grad}(f) \geq 1$ y $a - b \in K$, solo queda libre la opción $a - b = 0$. Es decir, $a = b$.

(3) Sea $f = \sum_{j=0}^{n} a_j x^j$. Entonces

$$f(a) = \sum_{j=0}^{n} a_j (x + (f))^j = \sum_{j=0}^{n} a_j (x^j + (f)) = \sum_{j=0}^{n} a_j x^j + (f) = f + (f) = 0.$$

(4) Sea $g + (f) \in L$ cualquiera, con $g = \sum_{j=0}^{m} a_j x^j$. Dado que

$$g + (f) = \sum_{j=0}^{m} a_j x^j + (f) = \sum_{j=0}^{m} a_j (x + (f))^j = \sum_{j=0}^{m} a_j a^j \in K(a),$$

se sigue que $L = K(a)$. Usando el teorema 5.2.6 (2) se tiene que

$$|L : K| = |K(a) : K| = \text{grad}(m_{a,K}) = \text{grad}(f)$$

con lo cual se tiene la afirmación. □

5.3.2 Corolario. Si $f \in K[x]$ es un polinomio no constante, entonces existe una extensión L de K con $|L : K| \leq \text{grad}(f)$, en la cual f tiene una raíz.

Demostración. Es suficiente descomponer a f en factores irreducibles y aplicar el teorema de Kronecker con uno de estos factores. □

5.3.3 Ejemplo. Sea $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Dado que $\text{grad}(f) = 2$ y f no se anula en $\mathbb{Z}_2$, se tiene que f es irreducible sobre $\mathbb{Z}_2$. Entonces, del teorema anterior se tiene que $\mathbb{Z}_2[x]/(f)$ es un cuerpo. Usando el algoritmo de la división con resto tenemos:

$$\mathbb{Z}_2[x]/(f) = \{g + (f) \mid \text{grad}(g) < 2\}.$$

En consecuencia,

$$\mathbb{Z}_2[x]/(f) = \{(f), 1 + (f), x + (f), x + 1 + (f)\}.$$

Para simplificar la notación, definamos $w := x + (f)$. Así

$$\mathbb{Z}_2[x]/(f) = \{0, 1, w, w + 1\}.$$

Las tablas de las operaciones en $\mathbb{Z}_2[x]/(f)$ son:

$+$	0	1	w	$w+1$
0	0	1	w	$w+1$
1	1	0	$w+1$	w
w	w	$w+1$	0	1
$w+1$	$w+1$	w	1	0

$\cdot$	0	1	w	$w+1$
0	0	0	0	0
1	0	1	w	$w+1$
w	0	w	$w+1$	1
$w+1$	0	$w+1$	1	w

5.3.4 Definición. Un cuerpo K se denomina `algebraicamente cerrado` si y solo si todo polinomio no constante $f \in K[x]$ tiene una raíz en K.

5.3.5 Ejemplo. El cuerpo de los números complejos es algebraicamente cerrado. (Teorema fundamental del álgebra).

5.3.6 Teorema. (Cuerpos algebraicamente cerrados) Las afirmaciones siguientes son equivalentes:

(1) K es algebraicamente cerrado.

(2) Todo polinomio no constante de $K[x]$ se descompone en factores lineales sobre K. Es decir, si $f \in K[x]$ no es constante, entonces existen $b, a_1, \ldots, a_n \in K$ tales que

$$f = b(x - a_1)\cdots(x - a_n).$$

(3) $f \in K[x]$ es irreducible sobre K si y solo si $\text{grad}(f) = 1$.

(4) No existe una extensión L/K algebraica con $L \neq K$.

(5) No existe una extensión L/K con $L \neq K$ y $|L : K| \in \mathbb{N}$.

Demostración. (1) $\Rightarrow$ (2). Supongamos que K es algebraicamente cerrado y sea $f \in K[x]$ no constante con $\text{grad}(f) = n$. Demostramos la afirmación por inducción matemática sobre n.

Sea $n = 1$. Por hipótesis se tiene que f tiene una raíz $a \in K$ y así $f = b(x - a)$ con $a, b \in K$.

Como hipótesis de inducción supongamos que si $\text{grad}(g) < n$, entonces

$$g = b(x - a_1)\cdots(x - a_k).$$

Finalmente, dado que f tiene una raíz en K, usando el algoritmo de la división se tiene que $f = (x - a_{k+1})g$ para algún $g \in K[x]$. Dado que $\text{grad}(g) = \text{grad}(f) - 1 < n$, podemos usar la hipótesis inductiva y se tiene que

$$(x - a_{k+1})g = b(x - a_1)\cdots(x - a_k)(x - a_{k+1}).$$

(2) $\Rightarrow$ (3). Evidente.

(3) $\Rightarrow$ (4). Sea L/K una extensión algebraica. Para probar (4) es suficiente demostrar que $L = K$. Es claro que $K \subseteq L$.

Recíprocamente, sea $a \in L$. Dado que a es algebraico sobre K, se tiene que $m_{a,K} = x - a \in K[x]$. Por lo tanto, $a \in K$.

(4) $\Rightarrow$ (5). Es inmediato ya que toda extensión finita es algebraica.

(5) $\Rightarrow$ (1). Sea $f \in K[x]$ no constante. Del corolario 5.3.2 se sigue que existe un cuerpo L y $a \in L$ tales que $K \subseteq L$ y $f(a) = 0$. Entonces, a es algebraico sobre K. Del teorema 5.2.9 se sigue que $K(a)/K$ es una extensión algebraica. Por lo tanto, $K(a) = K$ y se tiene que $a \in K$. Esto demuestra que K es algebraicamente cerrado. □

5.3.7 Definición. Un cuerpo $\overline{K}$ con $K \subseteq \overline{K}$ se denomina una `clausura algebraica` de K, si se verifican:

(1) $\overline{K}$ es algebraicamente cerrado.

(2) La extensión $\overline{K}/K$ es algebraica.

Sea L/K una extensión de cuerpos cualquiera. En el teorema 5.2.14 se demostró que $A := \mathrm{Alg}(L/K)$ es un cuerpo intermedio de L/K con la propiedad que A/K es algebraica. No obstante, no necesariamente es una clausura algebraica para K. Sin embargo, si L es un cuerpo algebraicamente cerrado, entonces el cuerpo intermedio A es una clausura algebraica de K, como se demuestra a continuación.

5.3.8 Lema. Sea K un cuerpo, $K \subseteq L$ y L algebraicamente cerrado. Entonces, $A := \mathrm{Alg}(L/K)$ es una clausura algebraica de K.

Demostración. Del teorema 5.2.14 se sigue que A/K es una extensión algebraica. Por lo tanto, resta demostrar solamente que A es algebraicamente cerrado.

Sea $f \in A[x]$ no constante. Dado que L es un cuerpo algebraicamente cerrado y $f \in L[x]$, podemos afirmar que f tiene una raíz $a \in L$. Entonces, a es algebraico sobre A. Dado que A/K es algebraica, del teorema 5.2.11 se sigue que a es algebraico sobre K. Por lo tanto, $a \in A$. Es decir, f tiene una raíz en A y del teorema 5.3.6 se sigue la afirmación. □

5.3.9 Ejemplos. (1) Del teorema fundamental del álgebra se tiene que $\mathbb{C}$ es un cuerpo algebraicamente cerrado. Además $\mathbb{C}$ es una clausura algebraica de $\mathbb{R}$.

(2) $\mathbb{C}$ no es una clausura algebraica de $\mathbb{Q}$, ya que $\mathbb{C}/\mathbb{Q}$ no es una extensión algebraica.

(3) El polinomio $f = x^2 + 1 \in \mathbb{Q}[x]$ no tiene raíces en $\mathrm{Alg}(\mathbb{R}/\mathbb{Q})$. Sus dos raíces están en la extensión $\mathrm{Alg}(\mathbb{C}/\mathbb{Q})$. No obstante, $\mathrm{Alg}(\mathbb{C}/\mathbb{Q})$ es una clausura algebraica de $\mathbb{Q}$. Sus elementos se denominan `números algebraicos`.

5.3.10 Teorema. (Ernst Steinitz, 1910) Todo cuerpo K tiene un clausura algebraica.

Demostración. Demostramos la existencia de la clausura algebraica de K utilizando el lema de Zorn. De la teoría de conjuntos se tiene que existe un conjunto infinito no enumerable S que contiene a K con $|K| < |S|$.

Sea $\mathcal{X}$ el conjunto de todas las extensiones L algebraicas sobre K que están contenidas en S. Dado que $K \in \mathcal{X}$, se verifica que $\mathcal{X} \neq \varnothing$. Definamos sobre $\mathcal{X}$ la siguiente relación:

$$A \leq B \Leftrightarrow A \text{ es subcuerpo de } B.$$

Se verifica sin dificultades que $\leq$ define una relación de orden parcial sobre $\mathcal{X}$.

(1) Toda cadena no vacía de $(\mathcal{X}, \leq)$ admite una cota superior.

En efecto, si $\mathcal{K}$ es una cadena no vacía de $(\mathcal{X}, \leq)$, entonces $T := \bigcup_{L \in \mathcal{X}} L$ es una cota superior para $\mathcal{K}$. Como consecuencia del lema de Zorn, se tiene que $(\mathcal{X}, \leq)$ admite un elemento maximal, digamos M.

(2) El elemento maximal M es algebraicamente cerrado.

Supongamos que M no es algebraicamente cerrado. Entonces, del teorema 5.3.6 se sigue que existe una extensión algebraica M' de M con $M' \neq M$. El cuerpo M' no podría no pertenecer a $\mathcal{X}$, ya que no necesariamente M' está contenido en S. Procedemos ahora a encontrar en S una imagen isomórfica de M'.

Por hipótesis S es un conjunto infinito no enumerable y $|K| < |S|$. Aplicando el lema 5.2.16 se sigue que

$$|M' \setminus M| \leq |M'| < |S| = |S \setminus M|.$$

Entonces, existe una función inyectiva

$$\varphi : M' \longrightarrow S$$

con $\varphi|_M = I_M$. Se verifica que φ es un isomorfismo de M' en $\varphi(M')$ con $\varphi|_M = I_M$ y, además, $\varphi(M')$ es una extensión algebraica de M con $\varphi(M') \neq M$. En efecto, si $a \in M'$ y $m_{a,M} = \sum_{j=0}^{n} m_j x^j$, entonces se verifica que

$$0 = \varphi\Big(\sum_{j=0}^{n} m_j a^j \Big) = \sum_{j=0}^{n} m_j \varphi(a)^j.$$

De la transitividad de la propiedad ser extensión algebraica (teorema 5.2.11 (2)) se sigue que $\varphi(M')$ es una extensión algebraica de K. Es decir, $\varphi(M') \in \mathcal{X}$. esto contradice

la maximalidad de M, por lo tanto nuestro supuesto es falso. Dado que M/K es una extensión algebraica, se sigue la afirmación. □

5.3.11 Ejemplo. Sea p número primo. Como consecuencia del teorema de Steinitz se verifica que $\mathbb{Z}_p$ admite una clausura algebraica. Demostramos que esta es infinita.

Supongamos que $\overline{\mathbb{Z}}_p$ es un cuerpo finito, digamos $|\overline{\mathbb{Z}}_p| = m$. Entonces, su grupo multiplicativo $\overline{\mathbb{Z}}_p^\times$ también lo es y, además, con orden $m-1$. En consecuencia,

$$a^{m-1} \equiv 1 \mod p, \quad \text{para todo } a \in \overline{\mathbb{Z}}_p^\times.$$

Es decir,

$$a^m - a = 0, \quad \text{para todo } a \in \overline{\mathbb{Z}}_p.$$

Como consecuencia, el polinomio

$$f = x^m - x + 1 \in \overline{\mathbb{Z}}_p[x]$$

no tiene raíces en $\overline{\mathbb{Z}}_p$. Es decir, $\overline{\mathbb{Z}}_p$ no es algebraicamente cerrado, lo cual es una contradicción.

5.3.12 Definición. Sean K_1 y K_2 cuerpos y $\varphi : K_1 \longrightarrow K_2$ un homomorfismo de cuerpos. Definimos la función

$$\hat{\varphi} : K_1[x] \longrightarrow K_2[x]$$

de la siguiente manera:

$$f = \sum_{i=0}^{n} k_i x^i \longmapsto \hat{\varphi}(f) = \sum_{i=0}^{n} \varphi(k_i) x^i.$$

Se verifica que $\hat{\varphi}$ es un homomorfismo y, además, $\hat{\varphi}(k) = \varphi(k)$ para todo $k \in K_1$.

5.3.13 Lema. Sean L_1/K_1 y L_2/K_2 extensiones de cuerpos, $\varphi : K_1 \longrightarrow K_2$ un isomorfismo, $f \in K_1[x]$ irreducible, $a \in L_1$ una raíz de f y $b \in L_2$ una raíz de $\hat{\varphi}(f)$. Entonces, existe un único monomorfismo

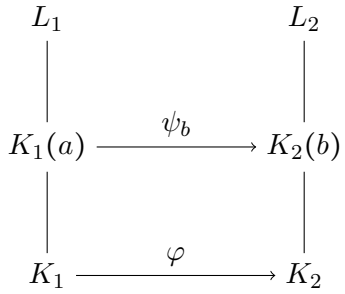
$$\psi_b : K_1(a) \longrightarrow L_2$$

con $\psi_b(k) = \varphi(k)$ para todo $k \in K_1$ y $\psi_b(a) = b$. Se verifica además que

$$\psi_b : K_1(a) \longrightarrow K_2(b)$$

es un isomorfismo.

Ilustración



DEMOSTRACIÓN. Dado que a es algebraico sobre K_1, del teorema 5.2.6 se sigue que

$$K_1(a) = \big\{g(a) \mid g \in K_1[x],\ \operatorname{grad}(g) < \operatorname{grad}(m_{a,K_1})\big\}.$$

(1) La existencia de ψ_b se garantiza de la siguiente manera: definamos

$$\psi_b : K_1(a) \longrightarrow L_2$$

mediante:

$$\psi_b(g(a)) = \hat{\varphi}(g)(b). \tag{5.4}$$

Es decir,

$$\psi_b\Big(\sum_{i=0}^{n} k_i a^i\Big) = \sum_{i=0}^{n} \varphi(k_i) b^i.$$

(2) Demostramos que ψ_b está bien definida. Supongamos que

$$g(a) = \sum_{i=0}^{n} k_i a^i = \sum_{i=0}^{n} t_i a^i = h(a) \tag{5.5}$$

con $g, h \in K_1[x]$. Recordemos que si $\operatorname{grad}(m_{a,K_1}) = n$, entonces

$$B = (1, a, \ldots, a^{n-1})$$

es una base para $K_1(a)$. Entonces, de (5.5) se sigue que $k_i = t_i$ y, en consecuencia,

$$\psi_b(g(a)) = \hat{\varphi}(g)(b) = \hat{\varphi}(h)(b) = \psi_b(h(a)).$$

(3) Demostramos que ψ_b es un homomorfismo de anillos. Sean $g(a), h(a) \in K_1(a)$ con $g, h \in K_1[x]$. Entonces,

$$\begin{aligned}
\psi_b(g(a) + h(a)) &= \psi_b((g+h)(a)) \\
&= \hat{\varphi}(g+h)(b) \\
&= (\hat{\varphi}(g) + \hat{\varphi}(h))(b) \\
&= \hat{\varphi}(g)(b) + \hat{\varphi}(h)(b) \\
&= \psi_b(g(a)) + \psi_b(h(a)).
\end{aligned}$$

Similar se demuestra que

$$\psi_b(g(a)h(a)) = \psi_b(g(a))\psi_b(h(a)).$$

(4) Dado que ψ_b no es idénticamente nula y $\ker(\psi_b)$ es un ideal de $K_1(a)$, se tiene que $\ker(\psi_b) = \{0\}$. Esto demuestra que ψ_b es inyectiva.

(5) Demostramos que $\mathrm{Im}(\psi_b) = K_2(b)$. Claramente $\mathrm{Im}(\psi_b) \subseteq K_2(b)$.

Recíprocamente, sea $w \in K_2(b)$. Entonces, existe $h = \sum_{i=0}^{n} t_i x^i \in K_2[x]$, que depende de w, tal que

$$w = \sum_{i=0}^{n} t_i b^i.$$

Por hipótesis se tiene que φ es biyectiva, por lo tanto,

$$w = \sum_{i=0}^{n} \varphi(k_i) b^i.$$

Si definimos $g = \sum_{i=0}^{n} k_i x^i$, entonces se tiene que $\hat{\varphi}(g)(b) = w$. Es decir, $\psi_b(g(a)) = w$.

(6) Si $k \in K_1$, entonces $\hat{\varphi}(k) \in K_2$. Por lo tanto,

$$\psi_b(k) = \hat{\varphi}(k)(b) = \hat{\varphi}(k) = \varphi(k).$$

(7) Demostramos que $\psi_b(a) = b$. Esto es inmediato, ya que

$$\psi_b(a) = \hat{\varphi}(x)(b) = x(b) = b.$$

(8) Demostramos la unicidad de ψ_b. Sea $\mu : K_1(a) \longrightarrow L_2$ un monomorfismo de anillos con $\mu(k) = \varphi(k)$ para todo $k \in K_1$ y $\mu(a) = b$.

Si $f = \sum_{i=0}^{n} k_i x^i$, entonces

$$0 = \mu(f(a)) = \mu\Big(\sum_{i=0}^{n} k_i a^i\Big) = \sum_{i=0}^{n} \varphi(k_i)\mu(a)^i = \hat{\varphi}(f)(\mu(a)).$$

Es decir, $\mu(a)$ es una raíz de $\hat{\varphi}(f)$.

Sea $u \in K(a)$, digamos $u = \sum_{i=0}^{m} u_i a^i$. Entonces,

$$\mu(u) = \sum_{i=0}^{m} \mu(u_i)\mu(a)^i = \sum_{i=0}^{m} \varphi(u_i) b^i = \psi_b(u).$$

Por lo tanto, $\mu = \psi_b$. □

5.3.14 Definición. Sean L_1/K y L_2/K extensiones del cuerpo K y

$$\sigma : L_1 \longrightarrow L_2$$

un homomorfismo de cuerpos. Si $\sigma\,|_K = I_K$, es decir $\sigma(k) = k$ para todo $k \in K$, entonces decimos que σ es un K-`homomorfismo`. Similar se definen K-`monomorfismo`, K-`isomorfismo` y K-`automorfismo`.

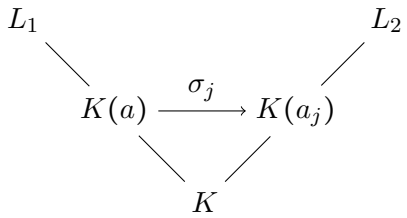
5.3.15 Observación. Sean L_1/K y L_2/K extensiones del cuerpo K y $a \in K$. Sea además $\sigma : K(a) \longrightarrow L_2$ un monomorfismo con $\sigma(k) = k$ para todo $k \in K$. Supongamos que

$$m_{a,K} = \prod_{j=1}^{n}(x - a_j),$$

con $a_j \in \overline{K}$ y $a_1 = a$. Entonces,

$$0 = \sigma(m_{a,K}(a)) = m_{a,K}(\sigma(a)).$$

Es decir, $\sigma(a) = a_j$ para algún j y se tiene que σ queda completamente determinado por las permutaciones de las raíces de $m_{a,K}$. Es decir, el número de K-monomorfismos coincide con el número de raíces distintas de $m_{a,K}$ y, a su vez, este es menor o igual que $\operatorname{grad}(m_{a,K})$.



5.3.16 Corolario. Sea L/K una extensión de cuerpos y $a, b \in L$ algebraicos sobre K. Entonces existe un K-monomorfismo

$$\psi : K(a) \longrightarrow L$$

con $\psi(a) = b$ si y solo si

$$m_{a,K} = m_{b,K}.$$

En este caso, ψ es un K-isomorfismo en $K(b)$ y, además,

$$\psi(f(a)) = f(b)$$

para todo $f \in K[x]$.

DEMOSTRACIÓN. Si $m_{a,K} = m_{b,K}$, entonces tanto a como b son raíces de $m_{a,K}$. Entonces, del lema anterior se garantiza la existencia del K-monomorfismo $\psi(a)$ con $\psi(a) = b$.

Recíprocamente, existe un K-monomorfismo $\psi : K(a) \longrightarrow L$ con $\psi(a) = b$, entonces

$$m_{a,K}(b) = m_{a,K}(\psi(a)) = \psi(m_{a,K}(a)) = 0.$$

En consecuencia, $m_{b,K} \mid m_{a,K}$. De la irreducibilidad de $m_{a,K}$ se sigue que $m_{a,K} = m_{b,K}$. □

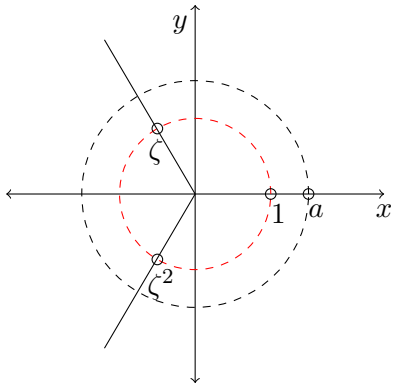
5.3.17 Ejemplos. (1) La función $\psi : \mathbb{C} \longrightarrow \mathbb{C}$ definida por $\psi(z) = \overline{z}$ es un $\mathbb{R}$-automorfismo.

(2) Dado que $m_{\mathrm{i},\mathbb{R}} = m_{-\mathrm{i},\mathbb{R}}$, el corolario anterior garantiza la existencia de un $\mathbb{R}$-isomorfismo $\psi : \mathbb{C} \longrightarrow \mathbb{C}$ con $\psi(\mathrm{i}) = -\mathrm{i}$. Este es la conjugación compleja.

(3) Sean ζ una raíz cúbica compleja de la unidad y $a = \sqrt[3]{2}$. Dado que $m_{a,\mathbb{Q}} = m_{a\zeta,\mathbb{Q}}$ se sigue que existe un $\mathbb{Q}$-monomorfismo

$$\psi : \mathbb{Q}(a) \longrightarrow \mathbb{Q}(a\zeta)$$

con $\psi(a) = a\zeta$.



(4) Si K es un cuerpo, entonces la función $\psi : K(x) \longrightarrow K(x)$ definida por

$$\psi\left(\tfrac{f}{g}\right) = \frac{f(x+1)}{g(x+1)}$$

es un K-automorfismo.

5.3.18 Teorema. (Unicidad de la clausura algebraica) Sean L/K una extensión algebraica y $\varphi : K \longrightarrow L_1$ un monomorfismo con L_1 un cuerpo algebraicamente cerrado. Entonces, existe un monomorfismo $\psi : L \longrightarrow L_1$ con $\psi|_K = \varphi$.

Demostración. Consideremos el conjunto $\mathcal{M}$ definido por

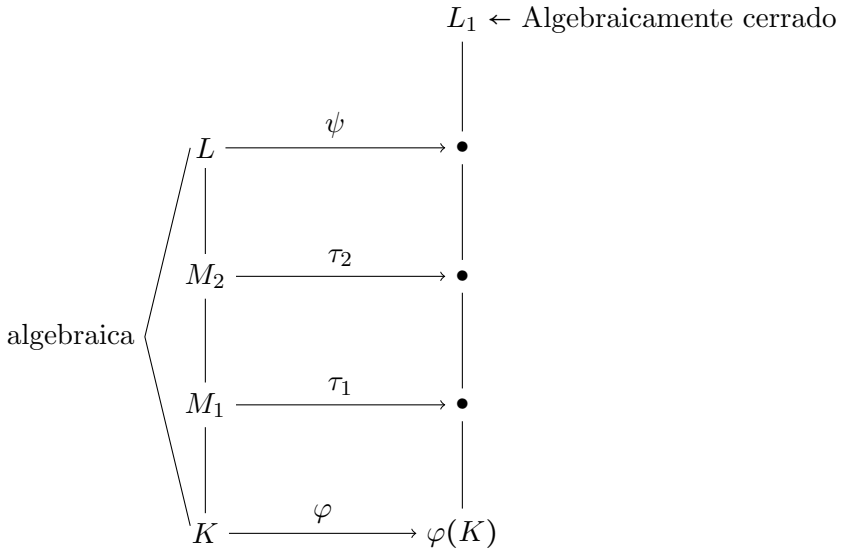
$$\mathcal{M} := \{(M, \tau) \mid K \subseteq M \subseteq L,\ \tau : M \longrightarrow L_1 \text{ monomorfismo y } \tau|_K = \varphi\}.$$

Dado que $(K, \varphi) \in \mathcal{M}$, se sigue que $\mathcal{M}$ es no vacío.

Definamos sobre $\mathcal{M}$ la siguiente relación:

$$(M_1, \tau_1) \leq (M_2, \tau_2) \Leftrightarrow M_1 \subseteq M_2 \ \wedge\ \tau_2|_{M_1} = \tau_1.$$

Se verifica sin dificultades que $\leq$ define un orden parcial sobre $\mathcal{M}$.



Sea $C = \{(M_j, \tau_j) \mid j \in \mathbb{N}\}$ una cadena de $\mathcal{M}$. Es decir, C es un conjunto totalmente ordenado. Si definimos

$$M' := \bigcup_{j \in \mathbb{N}} M_j$$

y

$$\tau'(a) := \tau_j(a) \text{ para todo } a \in M_j,$$

entonces (M', τ') es una cota superior para C. Por lo tanto, del lema de Zorn se sigue que $\mathcal{M}$ tiene un elemento maximal, digamos (M, τ).

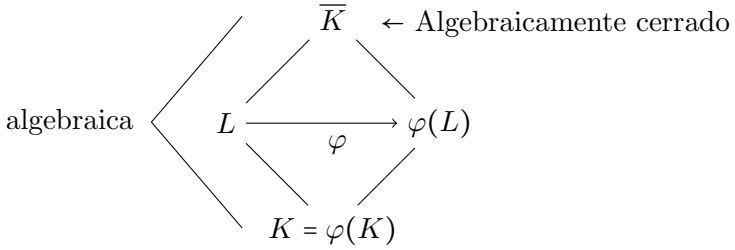
Demostramos ahora que $M = L$. Para ello, supongamos que $M \subset L$ y sea $a \in L \setminus M$. Entonces, a es algebraico sobre M y existe $m_a \in M[x]$.

Dado que L_1 es algebraicamente cerrado, se tiene que $\hat{\tau}(m_a)$ tiene una raíz $b \in L_1$. Si consideramos $\varphi : K \longrightarrow \varphi(K) \subseteq L_1$, entonces φ es un isomorfismo y del teorema 5.3.13

se sigue que existe un monomorfismo $\psi : M(a) \longrightarrow L_1$ con $\psi|_M = \tau$. Esto trae como consecuencia que $(M, \tau) < (M(a), \psi) \in \mathcal{M}$, lo cual contradice la maximalidad de M. En conclusión, $M = L$. □

5.3.19 Corolario. Sea $K \subseteq L \subseteq \overline{K}$ con $\overline{K}$ una clausura algebraica de K. Si $\varphi : L \longrightarrow \overline{K}$ es un monomorfismo con $\varphi(K) = K$, entonces existe un automorfismo $\psi : \overline{K} \longrightarrow \overline{K}$ con $\psi|_L = \varphi$.

Ilustración



Demostración. El teorema anterior garantiza la existencia de un monomorfismo ψ con tal propiedad. Resta demostrar que ψ es sobreyectiva.

Note que el cuerpo $\psi(\overline{K})$ es algebraicamente cerrado y $\overline{K}/\psi(\overline{K})$ es una extensión algebraica, ya que $\overline{K}/\varphi(K)$ lo es. Aplicando el teorema 5.3.6 se sigue que $\psi(\overline{K}) = \overline{K}$. □

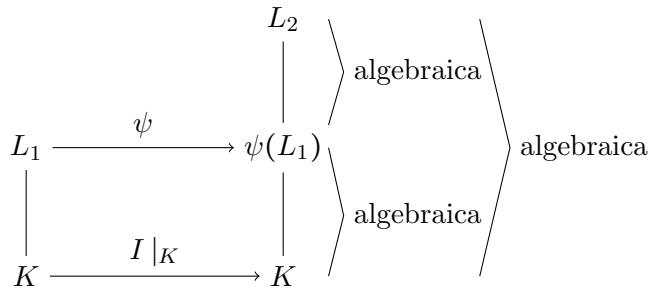
5.3.20 Corolario. Para toda extensión algebraica L/K existe un K-monomorfismo $\psi : L \longrightarrow \overline{K}$.

Demostración. Se sigue inmediatamente del teorema 5.3.18. □

En el siguiente teorema demostramos que, salvo K-isomorfía, la clausura algebraica de un cuerpo es única.

5.3.21 Teorema. Sea K un cuerpo. Si L_1 y L_2 son clausuras algebraicas de K, entonces L_1 y L_2 son isomorfas.

Ilustración



DEMOSTRACIÓN. Nuevamente del teorema 5.3.18 se sigue que existe un K-monomorfismo ψ de L_1 en L_2. Dado que las extensiones $L_2/\psi(L_1)$ y $\psi(L_1)/K$ son algebraicas, se sigue del teorema 5.3.6 que $\psi(L_1) = L_2$. Por lo tanto, ψ es un isomorfismo. □

5.4 Cuerpos de descomposición

5.4.1 Definición. Sean K un cuerpo y $f \in K[x]$ no constante. Una extensión L de K se denomina `cuerpo de descomposición` de f sobre K, si se verifican:

(1) f se descompone totalmente en $L[x]$. Es decir, existen $a, a_1, \ldots, a_n \in L$ tales que

$$f = a(x - a_1)\cdots(x - a_n).$$

(2) Si M es un cuerpo intermedio no trivial de L/K, entonces f no se descompone totalmente en $M[x]$.

Note que (2) es equivalente a:

(2)′ $L = K(a_1, \ldots, a_n)$, donde $a_1, \ldots, a_n \in L$ y son raíces de f.

De la definición se sigue que el cuerpo de descomposición de un polinomio f es el cuerpo más pequeño sobre el cual f se descompone totalmente. Además, dado que L/K es finitamente generada por elementos algebraicos, del teorema 5.2.9 se sigue que L/K es una extensión algebraica.

5.4.2 Ejemplos. (1) Sea $f = x^2 + 1 \in \mathbb{R}[x]$. Dado que

$$f = (x - \mathrm{i})(x + \mathrm{i})$$

y $\mathbb{R}(\mathrm{i}) = \mathbb{C}$, se tiene que $\mathbb{C}$ es un cuerpo de descomposición de f sobre $\mathbb{R}$.

(2) Sea $f = x^2 + 1 \in \mathbb{Q}[x]$. Entonces, $\mathbb{Q}(\mathrm{i})$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$.

(3) Sea $\zeta = \frac{-1\pm\sqrt{3}\mathrm{i}}{2}$ una raíz cúbica compleja de la unidad. Entonces, $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ es un cuerpo de descomposición de $f = x^3 - 2 \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$. En efecto, el conjunto A de las raíces de f está dado por

$$A = \{\sqrt[3]{2},\ \sqrt[3]{2}\zeta,\ \sqrt[3]{2}\zeta^2\}.$$

(4) Sea $f = x^4 + 1 \in \mathbb{Q}[x]$. Dado que

$$f = (x - \sqrt{\mathrm{i}})(x + \sqrt{\mathrm{i}})(x - \mathrm{i}\sqrt{\mathrm{i}})(x + \mathrm{i}\sqrt{\mathrm{i}}),$$

se verifica que $\mathbb{Q}(\mathrm{i}, \sqrt{\mathrm{i}}) = \mathbb{Q}(\sqrt{\mathrm{i}})$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$.

5.4.3 Teorema. (Existencia de cuerpos de descomposición) Todo polinomio no constante $f \in K[x]$ tiene un cuerpo de descomposición sobre K.

Demostración. Del teorema de Steinitz se sigue que K tiene una clausura algebraica, digamos $\overline{K}$, en la cual f puede descomponerse totalmente. Sea $A = \{a_1, \ldots, a_n\}$ el conjunto de raíces de f en $\overline{K}$. Entonces, $K(A)$ es un cuerpo de descomposición de f sobre K. □

En el siguiente teorema caracterizamos las extensiones de isomorfismos sobre cuerpos de descomposición.

5.4.4 Teorema. Sea $\varphi : K_1 \longrightarrow K_2$ un isomorfismo de cuerpos, $\hat{\varphi} : K_1[x] \longrightarrow K_2[x]$ como en la definición 5.3.12 y $f \in K_1[x]$ no constante. Sean, además, L_1 un cuerpo de descomposición de f sobre K_1 y L_2 un cuerpo de descomposición de $\hat{\varphi}(f)$ sobre K_2. Entonces:

(1) Si $\psi : L_1 \longrightarrow L_2$ es un monomorfismo con $\psi(k) = \varphi(k)$ para todo $k \in K_1$, entonces ψ es un isomorfismo. Además $c \in L_1$ es una raíz de f si y solo si $\psi(c)$ es una raíz de $\hat{\varphi}(f)$.

(2) Si g es un factor irreducible de f en $K_1[x]$, a es una raíz de g en L_1 y b es una raíz de $\hat{\varphi}(g)$ en L_2, entonces exite un isomorfismo $\psi : L_1 \longrightarrow L_2$ con $\psi(k) = \varphi(k)$ para todo $k \in K_1$ y $\psi(a) = b$.

Demostración.

(1) Es suficiente demostrar que ψ es sobre. Para ello supongamos que $f = a\prod_{j=1}^{n}(x - a_j)$ y $\hat{\varphi}(f) = b\prod_{j=1}^{n}(x - b_j)$. Dado que ψ es un homomorfismo de anillos y $\psi(k) = \varphi(k)$ para todo $k \in K_1$ se sigue que

$$\hat{\varphi}(f) = \hat{\psi}(f) = \psi(a)\prod_{j=0}^{n}(x - \psi(a_j)).$$

Por la unicidad de la descomposición de $\hat{\varphi}(f)$ se sigue que $(\psi(a_1), \ldots, \psi(a_n))$ es una permutación de $(b_1, \ldots, b_n)$. Por lo tanto,

$$\{b_1, \ldots, b_n\} \subseteq \mathrm{Im}(\psi). \tag{5.6}$$

Usando nuevamente el hecho que $\psi(k) = \varphi(k)$ para todo $k \in K_1$ tenemos que

$$K_2 = \varphi(K_1) = \psi(K_1) \subseteq \mathrm{Im}(\psi). \tag{5.7}$$

De (5.6) y (5.7) se sigue que

$$K_2(b_1, \ldots, b_n) \subseteq \mathrm{Im}(\psi).$$

Dado que L_2 es un cuerpo de descomposición de $\hat{\varphi}(f)$ sobre K_2 se tiene que

$$L_2 = K_2(b_1, \ldots, b_n) \subseteq \mathrm{Im}(\psi) \subseteq L_2.$$

Esto demuestra que $\mathrm{Im}(\psi) = L_2$ y se tiene que ψ es sobre.

Por otro lado, supongamos que $f = \sum_{j=0}^{n} a_j x^j$. Entonces,

$$\psi(f(c)) = \sum_{j=0}^{n} \psi(a_j)\psi(c)^j = \sum_{j=0}^{n} \varphi(a_j)\psi(c)^j = \hat{\varphi}(f)(\psi(c)).$$

Por lo tanto, dado que ψ es un monomorfismo

$$\begin{aligned} \psi(c) \text{ es una raíz de } \hat{\varphi}(f) &\Leftrightarrow \hat{\varphi}(f)(\psi(c)) = 0 \\ &\Leftrightarrow \psi(f(c)) = 0 \\ &\Leftrightarrow f(c) = 0 \\ &\Leftrightarrow c \text{ es una raíz de } f. \end{aligned}$$

(2) Demostramos la afirmación por inducción sobre $n := \mathrm{grad}(f)$.

Si $n = 1$, entonces $f = g$ es irreducible y podemos tomar $\psi = \varphi$.

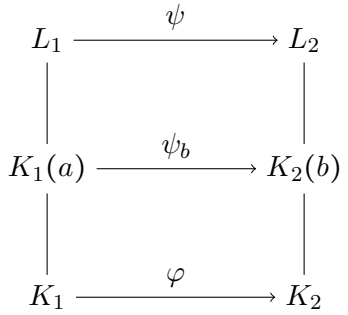
Como hipótesis inductiva, supongamos que la afirmación es válida para cualquier polinomio con grado menor que n.

Para concluir, sea $g = \sum_{j=0}^{t} b_j x^j \in K_1[x]$ un factor irreducible de f. Entonces, $\hat{\varphi}(g)$ es un divisor de $\hat{\varphi}(f)$.

Si $a \in L_1$ es una raíz de g y $b \in L_2$ es una raíz de $\hat{\varphi}(g)$, entonces del lema 5.3.13 se sigue que existe un isomorfismo

$$\psi_b : K_1(a) \longrightarrow K_2(b)$$

con $\psi_b(k) = \varphi(k)$ para todo $k \in K_1$ y $\psi_b(a) = b$.



Sean $f \in K_1(a)[x]$ y $\hat{\varphi}(f) \in K_2(b)[x]$ dados respectivamente por

$$f = (x-a)\sum_{j=0}^{n-1} c_j x^j \quad \text{y} \quad \hat{\varphi}(f) = (x-b)\sum_{j=0}^{n-1} \psi'(c_j)x^j.$$

Si definimos

$$g_1 := \sum_{j=0}^{n-1} c_j x^j \quad \text{y} \quad g_2 := \sum_{j=0}^{n-1} \psi'(c_j)x^j,$$

entonces L_1 y L_2 son cuerpos de descomposición de g_1 y g_2 sobre $K_1(a)$ y $K_2(b)$ respectivamente. Dado que $\operatorname{grad}(g_j) < n$ para $j = 1, 2$, por la hipótesis de inducción se sigue que existe un monomorfismo

$$\psi : L_1 \longrightarrow L_2$$

con $\psi|_{K(a)} = \psi_b$. El resto se sigue de (1). □

5.4.5 Corolario. (Ernst Steinitz, 1910) Si L_1 y L_2 son cuerpos de descomposición de $f \in K[x]$, entonces L_1 y L_2 son K-isomorfos.

Demostración. En el teorema anterior (2) tome $\varphi = I_K$. □

En el siguiente lema presentamos una cota superior para el grado de la extensión de un cuerpo de descomposición de un polinomio f.

5.4.6 Teorema. Sea $f \in K[x]$ de grado n. Si L es un cuerpo de descomposición de f sobre K, entonces $|L : K| \leq n!$.

Demostración. Procediendo por inducción matemática sobre n.

Si $n = 1$, entonces podemos suponer sin perder generalidad que $f = x - a \in K[x]$. En este caso, $L = K(a) = K$ y se tiene que $|L : K| = 1$.

Como hipótesis inductiva, supongamos que la afirmación es válida para cualquier polinomio g con $\text{grad}(g) < n$.

Sea $a \in L$ una raíz de f. De la división con resto se sigue que

$$f = (x - a)g$$

para algún $g \in K(a)[x]$ y L es un cuerpo de descomposición de g sobre $K(a)$. Dado que $\text{grad}(g) < \text{grad}(f)$, usando la hipótesis de inducción se tiene que

$$[L : K(a)| \leq (n-1)!.$$

Del teorema 5.2.6 y dado que $m_{a,K} \mid f$ se sigue que

$$\text{grad}(m_{a,K}) = |K(a) : K| \leq n.$$

Por lo tanto, aplicando la fórmula del grado se tiene que

$$|L : K| = |L : K(a)| \cdot |K(a) : K| \leq (n-1)!n = n!,$$

con lo cual se tiene la afirmación. □

Esta cota superior, además de ser una pésima, no puede mejorarse, en el sentido de acotar el grado con un número menor. Esto podemos apreciarlo en el siguiente ejemplo.

5.4.7 Ejemplo. Sea $f = x^3 - 2 \in \mathbb{Q}[x]$. Del ejemplo 5.4.2 (c) se tiene que $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ es un cuerpo de descomposición de f y

$$|\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}| = 6 = 3!.$$

5.4.8 Ejemplo. Sea $f = x^3 - 7 \in \mathbb{Q}[x]$. Usando el criterio de Eisenstein se sigue que f es irreducible sobre $\mathbb{Q}$. Note que

$$f = (x - \sqrt[3]{7})(x - \sqrt[3]{7}\zeta)(x - \sqrt[3]{7}\zeta^2),$$

donde ζ es una raíz cúbica compleja de la unidad.

Sean $a := \sqrt[3]{7}$, $b := a\zeta$ y $c := a\zeta^2$ y definamos $L := \mathbb{Q}(a, b, c)$. Del lema 5.3.13 se sigue que

$$\mathbb{Q}(a) \cong \mathbb{Q}(b) \cong \mathbb{Q}(c).$$

Dado que $\mathbb{Q}(a) \subseteq \mathbb{R}$ y $b, c \notin \mathbb{R}$ se sigue que $\mathbb{Q}(b) \neq \mathbb{Q}(a) \neq \mathbb{Q}(c)$.

Supongamos que $\mathbb{Q}(b) = \mathbb{Q}(c)$. Entonces, $\zeta = cb^{-1} \in \mathbb{Q}(b)$ y se tendría que $a = \zeta^{-1}b \in \mathbb{Q}(b)$. Por lo tanto, $\mathbb{Q}(a) \subseteq \mathbb{Q}(b)$. Dado que estos son isomorfos, se tendría que $\mathbb{Q}(a) = \mathbb{Q}(b)$, lo cual es una contradicción.

De lo anterior se tiene que $\mathbb{Q}(a) \neq \mathbb{Q}(b) \neq \mathbb{Q}(c)$. Entonces,

$$L = \mathbb{Q}(a,b,c) = \mathbb{Q}(a,b) = \mathbb{Q}(a,\zeta)$$

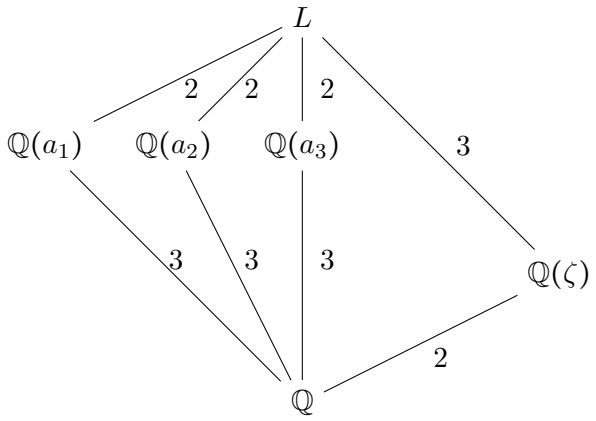
y se tiene que

$$|L:\mathbb{Q}| = |L:\mathbb{Q}(\zeta)| \cdot |\mathbb{Q}(\zeta):\mathbb{Q}| = 3 \cdot 2 = 6.$$

f `es irreducible en` $\mathbb{Q}(\zeta)[x]$. Si no lo fuese, entonces a o b o c sería una raíz de f en $\mathbb{Q}(\zeta)$, lo cual no es posible, como veremos a continuación:

Si $a_j \in \mathbb{Q}(\zeta)$, entonces $a = a_j\zeta^{j-1} \in \mathbb{Q}(\zeta)$. Por lo tanto, $\text{grad}(m_a) \leq 2$, lo cual no es posible, ya que $m_a \mid f$.

Ilustración.



5.5 Extensiones normales

Consideramos ahora extensiones algebraicas especiales.

5.5.1 Definición. Una extensión de cuerpos L/K se denomina `normal` si se verifican:

(1) L/K es algebraica.

(2) Todo polinomio irreducible sobre K, que tiene una raíz en L, se descompone totalmente en $L[x]$.

5.5.2 Ejemplo. Si $\overline{K}$ es la clausura algebraica de un cuerpo K, entonces trivialmente se verifica que $\overline{K}/K$ es una extensión normal.

5.5.3 Teorema. (Caracterización de extensiones normales) Sea $K \subseteq L$ una extensión de cuerpos finita y $\overline{L}$ la clausura algebraica de L, naturalmente también lo es de K. Son equivalentes:

(1) L/Kes normal.

(2) L es cuerpo de descomposición de algún $f \in K[x]$.

(3) Para todo K-monomorfismo $\psi : L \longrightarrow \overline{L}$ se verifica que $\psi(L) = L$. Es decir, ψ induce un K-automorfismo de L.

DEMOSTRACIÓN. (1) $\Rightarrow$ (2). Por hipótesis L/K es una extensión finita. Por lo tanto, del teorema 5.2.9 se sigue que $L = K(a_1, \ldots, a_n)$ con cada a_j algebraico sobre K.

Sea f_j el polinomio minimal de a_j sobre K. Entonces, cada f_j tiene una raíz en L y por hipótesis L/K es normal, por lo tanto, cada f_j se descompone en factores lineales en L.

(2) $\Rightarrow$ (3). Supongamos que L es cuerpo de decomposición de $f \in K[x]$. Entonces, $\psi(L)$ también es un cuerpo de descomposición de f. Del teorema 5.4.4 (1) se sigue que $\psi(L) = L$.

(3) $\Rightarrow$ (1). Dado que por hipótesis L/K es una extensión finita, nuevamente tenemos que L/K es algebraica.

Para concluir que L/K es normal, consideremos $f \in K[x]$ irreducible y sea $a \in L$ una raíz de f. Si $b \in \overline{L}$ es una raíz cualquiera de f, entonces del lema 5.3.12 se sigue que existe un K-monomorfismo

$$\psi' : K(a) \longrightarrow \overline{L}$$

con $\psi'(a) = b$. Del teorema 5.3.18 se sigue que ψ' puede extenderse a un K-monomorfismo

$$\psi : L \longrightarrow \overline{L}.$$

Aplicando la hipótesis (3) se sigue que $\psi(L) = L$ y, por lo tanto, $b \in L$. □

5.5.4 Ejemplos. Sea K un cuerpo.

(1) Si L/K es una extensión cuadrática, entonces L/K es normal.

En efecto, sea $a \in L \setminus K$ raíz de un polinomio irreducible $f \in K[x]$. De la fórmula del grado se sigue que

$$2 = |L : K| = \underbrace{|L : K(a)|}_{=1} \; |K(a) : K| = \operatorname{grad}(m_{a,K}).$$

Dado que $a \notin K$ se sigue que $L = K(a)$. Entonces, $\operatorname{grad}(f) = 2$ y

$$f = (x - a)(x - b)$$

para algún $b \in K(a) = L$. Esto trae como consecuencia que L es un cuerpo de descomposición de f sobre K.

(2) La propiedad `ser extensión normal` no es transitiva.

Sea $f = x^4 - 2 \in \mathbb{Q}[x]$. Aplicando el criterio de Eisenstein se tiene que f es irreducible sobre $\mathbb{Q}$. Las raíces de f están dadas por

$$\{\sqrt[4]{2}\, \mathrm{i}^k \mid k = 0, 1, 2, 3\}.$$

Entonces, $L = \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$ es un cuerpo de descomposición de f. Note que $f \in \mathbb{Q}[x]$ es el polinomio minimal de $\sqrt[4]{2}$ y así

$$|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = 4.$$

Similar se tiene que $h = x^2 - 2 \in \mathbb{Q}[x]$ es el polinomio minimal de $\sqrt{2}$ y, en consecuencia,

$$|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2.$$

Aplicando la fórmula del grado se tiene que

$$4 = |\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})|\ \underbrace{|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|}_{=2}.$$

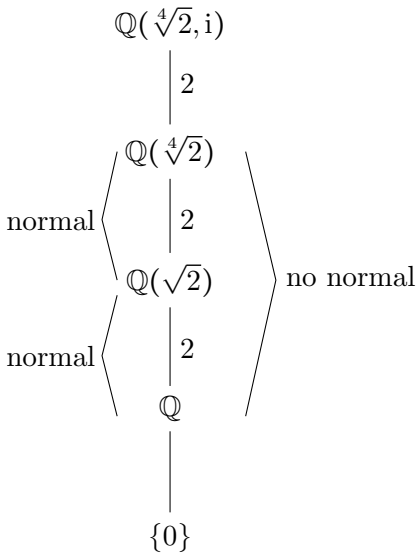
Por lo tanto, $|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})| = 2$.

Dado que las extensiones $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ son cuadráticas, de (1) se sigue que estas son extensiones normales.

`Afirmación.` La extensión $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es normal.

En efecto, $f = x^4 - 2 \in \mathbb{Q}[x]$ es el polinomio minimal de $\sqrt[4]{2}$ y f no se descompone totalmente en $\mathbb{Q}(\sqrt[4]{2})$, ya que $\sqrt[4]{2}\,\mathrm{i}$ es una raíz de f y $\sqrt[4]{2}\,\mathrm{i} \notin \mathbb{Q}(\sqrt[4]{2})$.

Finalmente, note que $\mathrm{i} \notin \mathbb{Q}(\sqrt[4]{2})$, por consiguiente, $x^2 + 1$ es el polinomio minimal de i sobre $\mathbb{Q}(\sqrt[4]{2})$. Por lo tanto, $|L : \mathbb{Q}(\sqrt[4]{2})| = 2$ y, en consecuencia, $|L : \mathbb{Q}| = 8$.



5.6 Extensiones separables

Iniciamos esta sección con el fenómeno de la `inseparabilidad`. Este consiste en que polinomios irreducibles sobre un cuerpo K pueden tener raíces múltiples en la clausura algebraica de K. Demostraremos que la `inseparabilidad` solo es posible para cuerpos de característica positiva.

5.6.1 Definición. Sea R un anillo conmutativo. Para $f = \sum_{j=0}^{n} a_j x^j \in R[x]$ se define la `derivada formal` de f, notada con f' de la siguiente manera

$$f' = \sum_{j=1}^{n} j a_j x^{j-1}.$$

5.6.2 Teorema. Sean $f, g \in R[x]$ y $r \in R$. Entonces:

(1) $(f+g)' = f' + g'$ y $(rf)' = rf'$.

(2) $(fg)' = f'g + fg'$.

(3) Si $\operatorname{grad}(f) > 0$, entonces $\operatorname{grad}(f') < \operatorname{grad}(f)$.

(4) Si $\operatorname{grad}(f) = 0$, entonces $f' = 0$.

Demostración. (1), (3) y (4) se siguen inmediatamente de la defnición de derivada. De la linealidad de la derivada, para demostrar (2), es suficiente considerar $g = x^m$.

Si $f = \sum_{j=0}^{n} a_j x^j$, entonces

$$\begin{aligned}(fg)' &= \Big(\sum_{j=0}^{n} a_j x^{m+j}\Big)' \\ &= \sum_{j=1}^{n}(m+j)a_j x^{m+j-1} \\ &= \Big(\sum_{j=1}^{n} j a_j x^{j-1}\Big)x^m + \Big(\sum_{j=0}^{n} a_j x^j\Big)(mx^{m-1}) \\ &= f'g + fg'. \quad \square\end{aligned}$$

5.6.3 Corolario. Sea $f = (x-a)^m g$ con $a \in R$ y $g \in R[x]$. Entonces,

$$f' = (x-a)^{m-1}(mg + (x-a)g').$$

Demostración. Usando la regla del producto, es suficiente demostrar que

$$((x-a)^m)' = m(x-a)^{m-1}.$$

Para ello escriba $(x-a)^m = (x-a)(x-a)^{m-1}$ y aplique la regla del producto e inducción matemática sobre m. $\square$

5.6.4 Definición. Sean L/K una extensión de cuerpos, $0 \neq f \in K[x]$, $m \in \mathbb{N}$ y $a \in L$. Decimos que a es una raíz `múltiple` de f si se verifican:

(1) $f = (x-a)^m g$

(2) $g(a) \neq 0$.

En este caso, $m \in \mathbb{N}$ se denomina la `multiplicidad` de a. Una raíz con multiplicidad 1 se denomina `simple`.

5.6.5 Ejemplo. $f = x^3 - 3x^2 + 4 = (x-2)^2(x+1) \in \mathbb{Q}[x]$ tiene una raíz simple y una raíz de multiplicidad 2.

5.6.6 Lema. Sea L un cuerpo de desomposición de $f \in K[x]$. Entonces,

(1) $a \in L$ es una raíz múltiple de f si y solo si $f(a) = 0 = f'(a)$.

(2) f tiene raíces múltiples en L si y solo si f y f' no son primos relativos. Es decir, tienen un divisor común no constante.

DEMOSTRACIÓN. (1) Si $a \in L$ es una raíz múltiple de f, entonces $(x-a)^2$ divide a f en $L[x]$. Es decir, $f = (x-a)^2 g$ para algún $g \in L[x]$. Entonces,

$$f' = (x-a)(2g + (x-a)g')$$

y se tiene que $f'(a) = 0$.

Recíprocamente, supongamos que a es una raíz simple de f. Es decir, $f = (x-a)g$, para algún $g \in L[x]$ con $g(a) \neq 0$. Entonces,

$$f' = (x-a)g' + g$$

y así $f'(a) = g(a) \neq 0$.

(2) Supongamos que f y f' son primos relativos. Es decir, $\mathrm{mcd}(f, f') = 1$. Entonces, existen $g, h \in K[x]$ tales que $gf + hf' = 1$. Por lo tanto, de (1) se sigue que f no tiene raíces múltiples.

Recíprocamente, supongamos que f y f' tienen un divisor común no constante, digamos $d \in K[x]$. Entonces, existe $a \in L$, el cual es una raíz de d. De (1) se sigue que a es una raíz múltiple de f. □

5.6.7 Ejemplos. (1) Sea $f = x^3 + 2x^2 + x + 2 \in \mathbb{Z}_3[x]$. Note que $f(1) = 0$. Por lo tanto, $f = (x-1)(x^2+1)$. Dado que $g = x^2 + 1$ es irreducible sobre $\mathbb{Z}_3$ y $g' = 2x \neq 0$ se tiene que no existen raíces múltiples en un cuerpo de descomposición de f.

(2) Sea $f = x^5 + 2x^4 + 2x^3 + 4x^2 + x + 2 \in \mathbb{Q}[x]$. Entonces,

$$f' = 5x^4 + 8x^3 + 6x^2 + 8x + 1.$$

Aplicando el algoritmo de Euclides se tiene que

$$\mathrm{mcd}(f, f') = x^2 + 1.$$

Por lo tanto, f tiene raíces múltiples. Se verifica que

$$f = (x^2+1)^2(x+2).$$

(3) Sean p un número primo y $K := \mathbb{Z}_p(x)$ el cuerpo de las funciones racionales sobre $\mathbb{Z}_p$. Entonces, $f = y^p - x \in K[y]$ es irreducible, es suficiente usar el criterio de Eisenstein, tomando como elemento primo sobre K a $x \in \mathbb{Z}_p[x]$. Dado que

$$f' = py^{p-1} = 0,$$

el polinomio irreducible f tiene raíces múltiples en un cuerpo de descomposición L.

5.6.8 Definición. Sea L/K una extensión de cuerpos. Un polinomio irreducible $f \in K[x]$ se denomina `separable` si f no admite raíces múltiples en $\overline{K}$. Un polinomio cualquiera $f \in K[x]$ se denomina separable si todos sus factores irreducibles lo son. En otro caso, f se denomina `inseparable`.

5.6.9 Ejemplos. (1) Si $a \in K$, entonces $f = x - a \in K[x]$ es separable.

(2) $f = (x^2+2)^3(x-3)^2(x^5+x^4+x^3+x^2+x+1) \in \mathbb{Q}[x]$ es separable.

(3) Si $f, g \in K[x]$ son separables, entonces $fg \in K[x]$ es separable.

(4) Sean p un número primo y $K := \mathbb{Z}_p(x)$ el cuerpo de las funciones racionales sobre $\mathbb{Z}_p$. Entonces, $f = y^p - x \in K[y]$ es inseparable.

En los siguientes resultados se demuestra que solo es posible encontrar polinomios inseparables en cuerpos de característica positiva.

5.6.10 Lema. Si $\mathrm{char}(K) = 0$, entonces todo $f \in K[x]$ es separable.

Demostración. Supongamos que $\mathrm{char}(K) = 0$ y sea $f \in K[x]$ no constante. Entonces, $f' \neq 0$ y del lema 5.6.6 (3) se sigue la afirmación. □

5.6.11 Teorema. Sea $f \in K[x]$ irreducible. Las siguientes afirmaciones son equivalentes:

(1) f es inseparable.

(2) $f' = 0$.

(3) $\mathrm{char}(K) = p$ y existe $f_1 \in K[x]$ tal que $f = f_1(x^p)$.

Demostración. (1) $\Rightarrow$ (2). Supongamos que f es inseparable y sea $a \in \overline{K}$ una raíz múltiple de f. Entonces, existen $g \in \overline{K}[x]$ y $m \in \mathbb{N}$ con $m > 1$ tales que

$$f = (x-a)^m g.$$

Del corolario 5.6.3 se sigue que $f'(a) = 0$. Dado que f es irreducible sobre K y $f(a) = 0$, se tiene que $f = m_{a,K}$. Es decir, f es el polinomio con menor grado para el cual a es una raíz. Dado, además, que $\mathrm{grad}(f') < \mathrm{grad}(f)$, se tiene que $f' = 0$.

(2) $\Rightarrow$ (3). Supongamos que $f' = 0$ y sea $f = \sum_{j=0}^{n} a_j x^j \in K[x]$ con $a_n \neq 0$ y $n > 0$. Entonces,

$$f' = \sum_{j=1}^{n} j a_j x^{j-1} = 0.$$

Se sigue entonces que $ja_j = 0$ para todo $j = 1, \ldots, n$ y, en particular, que

$$na_n = 0 \quad \text{con} \quad a_n \neq 0.$$

Esto demuestra que $\text{char}(K) = p$ para algún número primo p. De la condición $ja_j = 0$, se sigue que

$$a_j = 0 \quad \vee \quad p \mid j.$$

Por lo tanto, f tiene la forma

$$f = \sum_{i=0}^{k} a_{pi} x^{pi} = \sum_{i=0}^{k} a_{pi} (x^p)^i.$$

Si definimos $f_1 := \sum_{i=0}^{k} a_{pi} x^i$, entonces $f_1 \in K[x]$ y

$$f = f_1(x^p).$$

(3) $\Rightarrow$ (1). Supongamos que $f = \sum_{j=0}^{n} b_j (x^p)^j$ y sea $a \in \overline{K}$ una raíz de f. Aplicando el homomorfismo de Frobenius tenemos:

$$f = f - f(a) = \sum_{j=0}^{n} b_j ((x^p)^j - (a^p)^j) = \sum_{j=0}^{n} b_j (x^j - a^j)^p$$

y así a es una raíz de f con multiplicidad por lo menos p. Esto demuestra que f es inseparable. □

5.6.12 Teorema. Sea $f \in K[x]$ irreducible. Las siguientes afirmaciones son equivalentes:

(1) f es inseparable.

(2) $\text{char}(K) = p$ y existe $g \in K[x]$ irreducible y separable tal que

$$f = g(x^{p^m})$$

para algún $m \in \mathbb{N}$.

Demostración.

(1) $\Rightarrow$ (2). Supongamos que f es inseparable. Entonces, del teorema anterior se sigue que $\text{char}(K) = p$ y existe $f_1 \in K[x]$ tal que $f = f_1(x^p)$.

f_1 es irreducible sobre K, ya que, de lo contrario, con la sustitución $x \mapsto x^p$ se tendría que f es factorizable, lo cual no es posible por su irreducibilidad sobre K.

Para concluir la demostración, es suficiente probar que f_1 es separable. Supongamos que no lo es. Entonces, $f_1' = 0$. Dado que $\text{grad}(f_1) < \text{grad}(f)$, usando inducción sobre

el grado de f se sigue que $f_1(x) = g(x^{p^m})$ con lo cual $f(x) = g(x^{p^{m+1}})$ con un polinomio irreducible, separable $g \in K[x]$ y con $m \in \mathbb{N}$.

(2) $\Rightarrow$ (1). Sea $f = \sum_{j=0}^{n} b_j (x^{p^m})^j$ y sea $a \in \overline{K}$ una raíz de f. Entonces, aplicando el homomorfismo de Frobenius, tenemos:

$$f = f - f(a) = \sum_{j=0}^{n} b_j ((x^{p^m})^j - (a^{p^m})^j) = \sum_{j=0}^{n} b_j (x^j - a^j)^{p^m}$$

y así a es una raíz de f con multiplicidad por lo menos p^m. □

5.6.13 Definición. Sea L/K una extensión de cuerpos y $a \in L$.

(1) Se dice que a es `separable` sobre K si a es algebraico sobre K y su polinomio minimal $m_a \in K[x]$ es separable. En caso contrario, a se denomina `inseparable`.

(2) La extensión L/K se denomina `separable` si todo $a \in L$ es separable sobre K. Si en L existe un elemento inseparable sobre K, entonces decimos que la extensión L/K es `inseparable`.

5.6.14 Observación. Una extensión algebraica L/K es separable si y solo si para todo $a \in L$ el polinomio minimal $m_a \in K[x]$ tiene raíces simples en un cuerpo de descomposición.

5.6.15 Ejemplos. (1) Todo $a \in K$ es separable sobre K, ya que $m_{a,K} = x - a \in K[x]$ es separable.

(2) Una extensión cuadrática L/K es inseparable si y solo si $\mathrm{char}(K) = 2$ y existe $a \in L \setminus K$ con $a^2 \in K$.

Demostración. Supongamos que L/K es cuadrática e inseparable. Entonces, existe $a \in L \setminus K$ con

$$m_{a,K} = x^2 + bx + c \in K[x]$$

y

$$m'_{a,K} = 2x + b = 0,$$

con lo cual se tiene que $b = 0$ y $\mathrm{char}(K) = 2$.

Por otro lado, dado que $m_{a,K}(a) = 0$, se verifica que $a^2 = -c \in K$.

Recíprocamente, supongamos que $\mathrm{char}(K) = 2$ y existe $a \in L \setminus K$ con $a^2 \in K$. Dado que $f := x^2 - a^2 \in K[x]$ es irreducible sobre K y $f(a) = 0$, se tiene que $f = m_{a,K}$. Dado que $m_{a,K} = (x - a)^2 \in L[x]$ y así $a \in L$ es inseparable sobre K.

A la hora de obtener elementos inseparables, la característica del cuerpo juega un papel importante como veremos en el siguiente resultado.

5.6.16 Lema. Sea L/K una extensión de cuerpos y $a \in L$ algebraico sobre K.

(1) Si $\text{char}(K) = 0$, entonces a es separable.

(2) Si $\text{char}(K) = p > 0$, entonces a es separable sobre K si y solo si $K(a^p) = K(a)$.

Demostración.

(1) Se sigue del lema 5.6.10.

(2) Supongamos que a es separable sobre K. Del teorema 5.2.3 (4) se sigue que

$$m_{a,K(a^p)} \mid m_{a,K}.$$

Por lo tanto, a es separable sobre $K(a^p) \subseteq K(a)$.

Dado que a es raíz de

$$(x-a)^p = x^p - a^p \in K(a^p)[x],$$

del teorema 5.2.3 se sigue que

$$m_{a,K(a^p)} = x - a$$

con lo cual se tiene que $a \in K(a^p)$. En consecuencia, $K(a^p) = K(a)$.

Recíprocamente, supongamos que $\text{char}(K) = p > 0$ y a es inseparable sobre K. Entonces, del teorema 5.6.12 se sigue que existe un polinomio irreducible $f_1 \in K[x]$ tal que

$$m_{a,K} = f_1(x^p)$$

con $f_1(a^p) = 0$. Entonces,

$$|K(a^p) : K| = m_{a^p,K} \leq \text{grad}(f_1) < \text{grad}(m_{a,K}) = |K(a) : K|$$

y se sigue que $K(a^p) \neq K(a)$. □

En el siguiente lema demostramos que si a es un elemento algebraico sobre K, entonces siempre existe una potencia de a que es separable sobre K.

5.6.17 Lema. Sean K un cuerpo con $\text{char}(K) = p > 0$ y L una extensión de K. Si $a \in L$ es algebraico sobre K, entonces existe $m \in \mathbb{N}_0$ tal que a^{p^m} es separable sobre K.

Demostración. Si a es separable sobre K, entonces tomamos $m = 0$ y se tiene la afirmación.

Supongamos entonces, sin perder generalidad, que a es inseparable sobre K y procedemos por inducción matemática sobre $\text{grad}(m_{a,K}) = |K(a) : K|$.

Si $\operatorname{grad}(m_{a,K}) = 1$, entonces a es separable sobre K y la afirmacion se cumple. Del lema anterior podemos afirmar que

$$|K(a^p) : K| < |K(a) : K|.$$

Usando la hipótesis de inducción se sigue que existe $m \in \mathbb{N}_0$ tal que

$$a^{p^{m+1}} = (a^p)^{p^m}$$

es separable sobre K. □

5.6.18 Definición. Un cuerpo K se denomina `perfecto` si solo admite extensiones algebraicas separables. Es decir, todo $f \in K[x]$ es separable.

Los cuerpos `imperfectos` escasamente aparecen, como veremos en el siguiente teorema.

5.6.19 Teorema. (Ernst Steinitz) Sea K un cuerpo.

(1) Si $\operatorname{char}(K) = 0$, entonces K es perfecto.

(2) Si $\operatorname{char}(K) = p > 0$, entonces K es perfecto si y solo si el monomorfismo de Frobenius $\varphi(x) = x^p$ para todo $x \in K$ es sobreyectivo. Es decir, $K^p = K$.

(3) Todo cuerpo finito es perfecto.

Demostración.

(1) Se sigue inmediatamente del lema 5.6.16 (1).

(2) Supongamos que φ es sobreyectiva y sea $f \in K[x]$ irreducible. Si f fuese inseparable, entonces del teorema 5.6.11 se sigue que existe un polinomio $f_1 = \sum_{i=0}^{k} a_{ip} x^i \in K[x]$ tal que $f = f_1(x^p)$. Se tendría entonces que para todo $i = 1, \ldots, n$.

$$a_i = \varphi(b_i) = b_i^p, \quad \text{para algún } b_i \in K.$$

En consecuencia,

$$f = \sum_{i=0}^{k} b_i^p x^{ip} = \Big(\sum_{i=0}^{k} b_i x^i \Big)^p,$$

lo cual contradice la irreducibilidad de f.

Recíprocamente, supongamos que φ no es sobreyectiva y sea $b \in K \setminus K^p$. Sea a una raíz de $f = x^p - b \in K[x]$ en algún cuerpo de descomposición de f. Dado que $K = K(a^p) \subset K(a)$, del lema 5.6.16 (2) se sigue que a es inseparable sobre K.

(3) Se sigue de (2), ya que φ es inyectiva. □

5.6.20 Observaciones. Como consecuencia del teorema anterior tenemos:

(1) Los cuerpos no perfectos deben ser cuerpos infinitos con característica positiva.

(2) Sea $K = \mathbb{Z}_p(x)$ el cuerpo de las funciones racionales sobre $\mathbb{Z}_p$. Si $a := \sqrt[p]{t} \in \overline{K} \setminus K$, entonces el polinomio minimal $m_{a,K} \in K[x]$ está dado por

$$m_{a,K} = x^p - t.$$

Note que $m_{a,K} = (x-a)^p$, por lo tanto, a es inseparable sobre K.

5.6.21 Teorema. Sea L/K una extensión algebraica y separable. Si M es un cuerpo intermedio de L/K, entonces las extensiones L/M y M/K son separables.

Demostración. Se deja como ejercicio. □

5.6.22 Teorema. Si L/K es una extensión algebraica con $|L : K| = n$, entonces existen a lo más n K-monomorfismos $\sigma : L \longrightarrow \overline{K}$.

Demostración. Sean $L = K(a_1, \ldots, a_t)$ y $L_0 := K$. Para $i = 1, \ldots, t$ definamos $L_i := K(a_1, \ldots, a_i)$. Si $|L_i : L_{i-1}| = n_i$, entonces de la fórmula del grado se verifica que

$$n = \prod_{i=1}^{t} n_i.$$

Procedemos por inducción matemática sobre i. Si $i = 1$, entonces la afirmación se sigue inmediatamente del teorema 5.3.13.

Supongamos que para $i < t$ está demostrado que existen a lo más $\prod_{j=1}^{i} n_j$ K-monomorfismos de L_i en $\overline{K}$.

Dado que el polinomio minimal de a_{i+1} sobre L_i tiene grado n_{i+1}, se sigue del teorema 5.3.13 que cada uno de estos K-monomorfismo puede extenderse a un K-monomorfismos de L_{i+1} en $\overline{K}$ de a lo más n_{i+1} formas. Por lo tanto, existen a lo más

$$n_{i+1} \prod_{j=1}^{i} n_j$$

K-monomorfismos de L_{i+1} en $\overline{K}$ y se tiene la afirmación. □

5.6.23 Teorema. Sea L/K una extensión algebraica con $|L : K| = n$. Las siguientes afirmaciones son equivalentes:

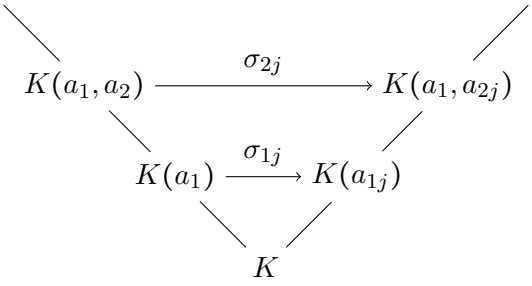
(1) L/K es separable.

(2) Existen exactamente n K-monomorfismos $\sigma : L \longrightarrow \overline{K}$.

DEMOSTRACIÓN. Dado que $|L : K| = n$, se sigue que $L = K(a_1, \ldots, a_t)$ con $t \leq n$. Para $i = 1, \ldots, t$ definamos como en el teorema anterior $L_i := K(a_1, \ldots, a_i)$. Supongamos que L/K es una extensión separable. Del teorema 5.6.21 se sigue que para cada $i = 1, \ldots, t-1$ la extensión L_{i+1}/L_i también es separable.

Sean $a_{j1}, \ldots, a_{jn_j}$ las raíces distintas de $m_{a_j,K}$ en $\overline{K}$. Del teorema 5.3.13 se sigue que existen n_j K-monomorfismos

$$\sigma_{ij} : L_i \longrightarrow \overline{K}$$



Un argumento similar como en el teorema anterior demuestra que existen n distintos K-monomorfismos de L en $\overline{K}$.

Recíprocamente, supongamos que L/K es inseparable y sea a_1 un elemento inseparable sobre K. Entonces, $m_{a_1,K} \in K[x]$ tiene menos de n_1 raíces distintas, donde $n_1 := \text{grad}(m_{a_1,K})$. Nuevamente del teorema 5.3.13 se sigue que existen menos de n_1 K-monomorfismos de L_1 en $\overline{K}$. Esta pérdida no es posible recuperarla cuando extendemos el argumento hacia L. Por lo tanto, existen menos de n K-homomorfismos de L en $\overline{K}$. □

5.6.24 Corolario. Sea $L = K(a_1, \ldots, a_t)$, donde para cada $i = 1, \ldots, t$ se verifica que a_i es separable sobre $L_i = K(a_1, \ldots, a_{i-1})$. Entonces, L/K es separable.

DEMOSTRACIÓN. Del teorema anterior se sigue que existen $|L : K|$ distintos K-homomorfismos de L en $\overline{K}$ con lo cual se concluye que L/K es separable. □

5.6.25 Corolario. (Transitividad de la separabilidad) Sea M un cuerpo intermedio de la extensión L/K. Si L/M y M/K son extensiones separables, entonces L/K es separable.

DEMOSTRACIÓN. Sea $a \in L$. Demostramos que a es separable sobre K. Sea

$$m_{a,M} = x^n + \cdots + a_1 x + a_0 \in M[x].$$

Si definimos $M' := K(a_0, \ldots, a_{n-1})$, entonces a es separable sobre M' y del teorema 5.6.21 se sigue que M' es separable sobre K. Del corolario anterior se tiene que $M'(a)$ es separable sobre K, por lo tanto, a en particular también lo es. □

5.6.26 Teorema. (Existencia de elementos primitivos) Si L/K es una extensión separable y finita, entonces existe un elemento primitivo. Es decir, existe $a \in L$ tal que $L = K(a)$.

DEMOSTRACIÓN. Si K es finito, entonces L también lo es. Por lo tanto, podemos tomar como elemento primitivo al elemento generador del grupo multiplicativo $L^\times$.

Supongamos entonces, sin perder generalidad, que K y L son infinitos. Sea $L = K(a_1, \ldots, a_n)$. Demostramos la afirmación por inducción sobre n.

Si $n = 1$, entonces el resultado es inmediato.

Supongamos que $K(a_1, \ldots, a_{n-1}) = K(c)$. Si definimos $b := a_n$, entonces es suficiente demostrar que $K(b, c) = K(a)$ para algún $a \in L$. Es decir, es suficiente demostrar la existencia de elementos primitivos para $n = 2$.

Sean $\psi_1, \ldots, \psi_s$ los distintos K-isomorfismos definidos de $K(b, c)$ en $\overline{K}$, garantizados por el teorema 5.6.23. Definamos el polinomio f mediante

$$f := \prod_{j \neq i} (\psi_i(c) - \psi_j(c))x + (\psi_i(b) - \psi_j(b)).$$

Si f fuese idénticamente nulo, entonces $\psi_i(c) = \psi_j(c)$ para todo $i, j = 1, \ldots, s$ y $\psi_k(b) = \psi_r(b)$ para algunos $r, k \in \{1, \ldots, s\}$. Esto traería como consecuencia que $\psi_k = \psi_r$. (Recuerde que los isomorfismos ψ_j quedan completamente determinados por la acción de estos sobre los generadores). Por lo tanto, f no es idénticamente nulo y existe $a \in K$ tal que $f(a) \neq 0$.

Dado que $a \in K$ se verifica que $\psi_i(ac + b) \neq \psi_j(ac + b)$ para $i \neq j$ y, consecuentemente,

$$|K(ac + b) : K| = \operatorname{grad}(m_{ac+b}) \geq s.$$

Del teorema 5.6.23 se sigue que $|K(b, c) : K| = s$. Dado que tenemos la cadena

$$K \subseteq K(ac + b) \subseteq K(b, c)$$

se sigue que $K(ac + b) = K(b, c)$. □

5.7 El teorema fundamental de la teoría de Galois

5.7.1 Definición. Sea L/K una extensión de cuerpos. Notamos con $\mathrm{Aut}(L/K)$ al conjunto de todos los K-isomorfismos de L. Esto es

$$\mathrm{Aut}(L/K) := \{\sigma \mid \sigma \in \mathrm{Aut}(L),\ \sigma(x) = x,\ \forall x \in K\}.$$

Se verifica que $\mathrm{Aut}(L/K)$ con la composición de funciones es un grupo. En efecto, es claro que $\mathrm{Aut}(L/K) \subseteq \mathrm{Aut}(L)$ y si $\beta \in \mathrm{Aut}(L/K)$ y $x \in K$, entonces

$$x = \beta^{-1}(\beta(x)) = \beta^{-1}(x).$$

En consecuencia, para todo $\alpha, \beta \in \mathrm{Aut}(L/K)$ se tiene que

$$\alpha\beta^{-1}(x) = \alpha(\beta^{-1}(x)) = \alpha(x) = x.$$

$\mathrm{Aut}(L/K)$ se llama el `grupo de automorfismos` de L sobre K.

5.7.2 Observaciones. (1) Si P es el cuerpo primo de K, entonces $\mathrm{Aut}(K/P) = \mathrm{Aut}(K)$.

(2) Del teorema 5.6.22 se sigue que si L/K es una extensión algebraica con $|L : K| = n$, entonces $|\mathrm{Aut}(L/K)| \leq n$. Es decir $\mathrm{Aut}(L/K)$ es un grupo finito.

5.7.3 Lema. Sea $f \in K[x]$ no constante y L un cuerpo de descomposición de f sobre K. Supongamos que

$$f = \prod_{j=1}^{n} (x - a_j)^{c_j}$$

con $a_i \neq a_j$ para $i \neq j$. Entonces,

(1) Para $A = \{a_1, \ldots, a_n\}$ la función $\tau : \mathrm{Aut}(L/K) \longrightarrow \mathrm{Sym}(n)$ definida por

$$\tau(\sigma) = \sigma|_A$$

es un monomorfismo. En particular, $\mathrm{Aut}(L/K)$ es isomorfo a un subgrupo de $\mathrm{Sym}(n)$ y, además, queda determinado de manera única por las permutaciones de las raíces de f.

(2) Si f es irreducible, entonces $\mathrm{Aut}(L/K)$ actúa transitivamente sobre A. Es decir, para cada par de elementos $a_i, a_j \in A$ existe $\sigma \in \mathrm{Aut}(L/K)$ tal que $\sigma(a_i) = a_j$.

(3) Si para cada $j \in \{1, \ldots, n\}$ se verifica que $c_j = 1$ y $\mathrm{Aut}(L/K)$ actúa transitivamente sobre A, entonces f es irreducible sobre K.

Demostración.

(1) Sea $\sigma \in \mathrm{Aut}(L/K)$. Se verifica que $\sigma(A) \subseteq A$. En efecto,

$$f(\sigma(a_j)) = \sigma(f(a_j)) = \sigma(0) = 0.$$

Dado que σ es inyectiva y A es finito, se sigue que $\sigma(A) = A$. Es decir, $\sigma|_A \in \mathrm{Sym}(n)$.

Demostramos ahora que τ es un monomorfismo. Dado que $L = K(a_1, \ldots, a_n)$ se tiene que

$$\begin{aligned} \sigma \in \ker(\tau) &\Leftrightarrow \sigma|_A = I_A \\ &\Leftrightarrow \sigma = I_L. \end{aligned}$$

(2) Se sigue del teorema 5.4.4.

(3) Supongamos que $c_j = 1$ para todo $j \in \{1, \ldots, n\}$ y que $\mathrm{Aut}(L/K)$ actúa transitivamente sobre A. Para demostrar la irreducibilidad de f supongamos además que $f = gh$ con $g, h \in K[x]$ no constantes. Sin perder generalidad, supongamos que a_1 es una raíz de g y a_n lo es de h. Entonces, existe $\sigma \in \mathrm{Aut}(L/K)$ tal que $\sigma(a_1) = a_n$. Note que si $g = \sum_{j=0}^{n} b_j x^j \in K[x]$, entonces

$$\hat{\sigma}(g) = \sum_{j=0}^{n} \sigma(b_j) x^j = \sum_{j=0}^{n} b_j x^j = g.$$

Por lo tanto, del teorema 5.4.4 se sigue que $\sigma(a_1)$ es una raíz de $\hat{\sigma}(g) = g$, pero $\sigma(a_1)$ es una raíz de h, lo cual contradice la simplicidad de las raíces de f. □

5.7.4 Ejemplo. Sea $f = x^3 - 7 \in \mathbb{Q}[x]$. Del ejemplo 5.4.8 se tiene que

$$L = \mathbb{Q}(a_1, a_1\zeta, a_1\zeta^2) = \mathbb{Q}(a_1, \zeta),$$

donde $a_1 = \sqrt[3]{7}$ y ζ es una raíz cúbica compleja de la unidad. L es un cuerpo de descomposición de f. Además

$$|L : \mathbb{Q}| = 6.$$

Del lema 5.7.3 se sigue que $G := \mathrm{Aut}(L/\mathbb{Q})$ es isomorfo a un subgrupo de $\mathrm{Sym}(3)$. Dado que f es irreducible sobre $\mathbb{Q}$ se sigue que G actúa transitivamente sobre $A = \{a_1, a_1\zeta, a_1\zeta^2\}$. Es claro que $L \subseteq \mathbb{C}$ y que $\sigma(z) = \bar{z}$ es un automorfismo de $\mathbb{C}$. Del teorema 5.5.3 se sigue que $\sigma|_L \in G$. Dado que $a_1 \in \mathbb{R}$, se sigue que

$$\sigma|_A = (a_1\zeta, a_1\zeta^2).$$

Es claro que G actúa transitivamente sobre A: por lo tato existe $\tau \in G$ tal que $\tau(a_1) = a_1\zeta$. Para determinar completamente a τ consideramos todos los casos posibles.

Caso 1. $\tau(a_1\zeta^2) = a_1\zeta^2$. Entonces se verifica que

$$\sigma|_A \circ \tau = (a_1, a_1\zeta^2, a_1\zeta) \in G.$$

Caso 2. $\tau(a_1\zeta^2) \neq a_1\zeta^2$. Entonces, τ es 3-ciclo.

Dado que Sym(3) es generado por una involución y un 3-ciclo, podemos afirmar que $\mathrm{Aut}(L/\mathbb{Q}) \cong \mathrm{Sym}(3)$.

$$\mathrm{Aut}(L/\mathbb{Q}) = \{\sigma_0, \ldots, \sigma_5\},$$

donde σ_j está dado por

$$a_1 \longmapsto a_1\zeta^j, \quad \zeta \longmapsto \zeta, \quad (j = 0, 1, 2)$$

y

$$a_1 \longmapsto a_1\zeta^j, \quad \zeta \longmapsto \zeta^2, \quad (j = 0, 1, 2).$$

5.7.5 Definición. Una extensión de cuerpos finita L/K se denomina `extensión de Galois` si y solo si L/K es normal y separable. En este caso, $\mathrm{Aut}(L/K)$ se denomina `grupo de Galois` de la extensión y se nota con $\mathrm{Gal}(L/K)$.

5.7.6 Observación. Si L/K es una extensión separable, entonces el número de K-monomorfismos es igual a $|L : K|$. Ver teorema 5.6.23.

Si L/K es una extensión normal, entonces todos los $a_j \in L$ y así K-monomorfismo equivale a K-isomorfismo.

5.7.7 Teorema. Sea L/K una extensión de cuerpos. Las siguientes afirmaciones son equivalentes:

(1) L/K es una extensión de Galois.

(2) L es cuerpo de descomposición de algún polinomio separable en $K[x]$.

(3) $|L : K| \in \mathbb{N}$ y $|\mathrm{Gal}(L/K)| = |L : K|$.

Demostración. (1) $\Rightarrow$ (2). Si L/K es una extensión de Galois, entonces $L = K(a_1, \ldots, a_n)$ con $a_j \in L$. Los polinomios minimales $m_{a_j,K}$ son separables sobre K y L es cuerpo de descomposición del polinomio

$$f = \prod_{j=1}^{n} m_{a_j,K}.$$

(2) $\Rightarrow$ (1). Si $f \in K[x]$ es separable, entonces el cuerpo de descomposición L de f es claramente separable. Es inmediato que L/K es normal, por lo tanto L/K es una extensión de Galois.

(1) $\Leftrightarrow$ (3). Sea $\overline{L}$ la clausura algebraica de L. Cada $\sigma \in \mathrm{Aut}(L/K)$ puede considerarse como un K-homomorfismo $\sigma : L \longrightarrow \overline{L}$.

Si definimos $n := |L : K|$, entonces del teorema 5.6.23 se sigue que L/K es separable si y solo si existen exactamente n K-monomorfismos $\tau : L \longrightarrow \overline{L}$. Del teorema 5.5.3 se tiene que L/K es normal si y solo si $\tau(L) = L$ para cada uno de estos τ. $\square$

5.7.8 Corolario. Sea L/K una extensión de cuerpos.

(1) Si $\mathrm{char}(K) = 0$, entonces las extensiones de Galois de K son los cuerpos de descomposición de polinomios en $K[x]$.

(2) Si M es un cuerpo intermedio de L/K, entonces L/M es una extensión de Galois y $\mathrm{Gal}(L/M)$ es un subgrupo de $\mathrm{Gal}(L/K)$.

5.7.9 Ejemplo. Sea $f = x^2 - 2 \in \mathbb{Q}[x]$. Note que $L = \mathbb{Q}(\sqrt{2})$ es un cuerpo de descomposición de f y así la extensión $L/\mathbb{Q}$ es de Galois con $|L : \mathbb{Q}| = 2$. Del teorema anterior se sigue que $|\mathrm{Gal}(L/\mathbb{Q})| = 2$.

Si $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, entonces

$$2 = \sigma(2) = \sigma(\sqrt{2}^2) = \sigma(\sqrt{2})^2.$$

En consecuencia,

$$\sigma(\sqrt{2}) = \pm\sqrt{2}.$$

Por otro lado,

$$\sigma^2(\sqrt{2}) = \sigma(\pm\sqrt{2}) = \sqrt{2}.$$

En consecuencia, $\sigma^2 = I_L$ y se tiene que

$$\mathrm{Gal}(L/\mathbb{Q}) = \{I_L, \sigma_1\},$$

donde σ_1 es la función conjugación. Esto es,

$$\sigma_1(x + y\sqrt{2}) = x - y\sqrt{2}.$$

Es evidente que $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo a $\mathbb{Z}_2$.

En general, si $d \in \mathbb{Z}$ y d no es un cuadrado, entonces la extensión $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ tiene exactamente dos $\mathbb{Q}$-automorfismos: la idéntica y la conjugación.

5.7.10 Ejemplo. Sea $f = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. Note que

$$f = (x^2 - 2)(x^2 - 3)$$

y el cuerpo de descomposición de f está dado por

$$L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Si definimos $a := \sqrt{2} + \sqrt{3}$, entonces $m_{a,\mathbb{Q}} = x^4 - 10x + 1$. Por lo tanto, $|L : \mathbb{Q}| = 4$ y del teorema 5.7.7 se sigue que $|\mathrm{Gal}(L/\mathbb{Q})| = 4$.

Si $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, entonces

$$2 = \sigma(2) = \sigma(\sqrt{2}^2) = \sigma(\sqrt{2})^2.$$

En consecuencia,

$$\sigma(\sqrt{2}) = \pm\sqrt{2}.$$

De manera similar se obtiene que

$$\sigma(\sqrt{3}) = \pm\sqrt{3}.$$

Por otro lado,

$$\sigma^2(\sqrt{2}) = \sigma(\pm\sqrt{2}) = \sqrt{2}$$

y

$$\sigma^2(\sqrt{3}) = \sigma(\pm\sqrt{3}) = \sqrt{3}.$$

En consecuencia, $\sigma^2 = I_L$ y se tiene que

$$\mathrm{Gal}(L/\mathbb{Q}) = \{I_L = \sigma_1, \sigma_2, \sigma_3, \sigma_4\},$$

donde

	σ_1	σ_2	σ_2	σ_4
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$-\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$

Es claro que $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo al 4-grupo de Klein.

5.7.11 Ejemplo. Dado que $\mathbb{C}/\mathbb{R}$ es una extensión cuadrática y $\mathrm{char}(\mathbb{R}) = 0$, se tiene que $\mathbb{C}/\mathbb{R}$ es una extensión normal y separable. Por lo tanto, $\mathbb{C}/\mathbb{R}$ es una extensión de Galois y se tiene que $|\mathrm{Aut}(\mathbb{C} : \mathbb{R})| = 2$. No es difícil demostrar que

$$\mathrm{Aut}(\mathbb{C} : \mathbb{R}) = \{I_{\mathbb{C}}, z \mapsto \bar{z}\}.$$

El tema central de esta sección es establecer conexiones entre los subgrupos de $\mathrm{Aut}(L/K)$ y los cuerpos intermedios de L/K.

5.7.12 Teorema. Sean K y L cuerpos y $\sigma_1, \ldots, \sigma_n$ isomorfismos de K en L distintos. Sean $a_1, \ldots, a_n \in L$ dados tales que

$$\sum_{j=1}^{n} a_j \sigma_j(x) = 0 \quad \text{para todo } x \in K. \tag{5.8}$$

Entonces, $a_1 = a_2 = \cdots = a_n = 0$.

Demostración. Procedemos por inducción sobre n.

Si $n = 1$, entonces $a_1\sigma_1(x) = 0$ para todo $x \in K$. Si tomamos $x = 1$, entonces se tiene $a_1 = 0$.

Sea $n > 1$ y supongamos que la afirmación es válida para $n - 1$.

Supongamos que se tiene (5.8). Dado que $\sigma_n \neq \sigma_1$ existe $y \in K$ tal que $\sigma_n(y) \neq \sigma_1(y)$. Multiplicando (5.8) por $\sigma_n(y)$ tenemos

$$\sum_{j=1}^{n} a_j \sigma_j(x)\sigma_n(y) = 0 \quad \text{para todo } x \in K \tag{5.9}$$

Dado que cada σ_j es en particular un homomorfismo de anillos, al reemplazar en (5.8) x por xy tenemos

$$\sum_{j=1}^{n} a_j \sigma_j(x)\sigma_j(y) = 0 \quad \text{para todo } x \in K \tag{5.10}$$

Restando miembro a miembro (5.9) y (5.10) se tiene

$$a_1(\sigma_n(y) - \sigma_1(y))\sigma_1(x) + \cdots + a_{n-1}(\sigma_n(y) - \sigma_{n-1}(y))\sigma_{n-1}(x) = 0$$

para todo $x \in K$. Dado que $\sigma_n(y) \neq \sigma_1(y)$, la hipótesis de inducción suministra $a_1 = 0$. Aplicando ahora la hipótesis de inducción en (5.8) se verifica que $a_2 = \cdots = a_n = 0$. □

5.7.13 Definición. Sean L un cuerpo y U un subgrupo finito de $\mathrm{Aut}(L)$. La función $T_U : L \longrightarrow L$ definida por

$$T_U(x) := \sum_{\sigma \in U} \sigma(x)$$

se denomina la U-`traza` sobre L.

5.7.14 Teorema. (Emil Artin) Sean L un cuerpo, U un subgrupo finito de $\mathrm{Aut}(L)$ y K el conjunto de los elementos de L que son U-`invariantes`. Es decir,

$$K := \{x \in L \mid \sigma(x) = x, \ \forall \sigma \in U\}.$$

Entonces,

(1) K es un subcuerpo de L.

(2) $|L : K| = |U|$.

(3) $\mathrm{Aut}(L/K) = U$.

(4) L/K es una extensión de Galois y $\mathrm{Gal}(L/K) = U$.

DEMOSTRACIÓN. Supongamos que $U = \{\sigma_1, \ldots, \sigma_n\}$. Es decir, $|U| = n$.

(1) Claramente $0, 1 \in K$. Dado que cada σ_j es un automorfismo de L, se verifica inmediatamente que K es un subcuerpo de L.

(2) Si consideramos a L como espacio vectorial sobre K se tiene que cada σ_j es una función K-lineal. En efecto, si $x \in L$ y $k \in K$, entonces

$$\sigma_j(kx) = \sigma_j(k)\sigma_j(x) = k\sigma_j(x).$$

Por otro lado, si $x \in L$, entonces para todo $j = 1, \ldots, n$ se verifica que

$$\sigma_j(T_U(x)) = \sum_{i=1}^{n} \sigma_j(\sigma_i(x)) = \sum_{k=1}^{n} \sigma_k(x) = T_U(x).$$

Esto demuestra que $T_U(x) \in K$. Del teorema 5.7.12 se sigue que existe por lo menos un $x \in L$ tal que $T_U(x) \neq 0$.

Supongamos que $|L : K| = r < n$ y sea $B = (w_1, \ldots, w_r)$ una K-base para L. El sistema de ecuaciones lineales

$$\sum_{i=1}^{n} \sigma_i(w_k)x_i = 0, \text{ con } k = 1, \ldots, r$$

admite una solución no trivial, digamos $(a_1, \ldots, a_n) \in L^n$. Es decir, existe $a_j \neq 0$ con $1 \leq j \leq n$ tal que

$$\sum_{i=1}^{n} \sigma_i(w_k)a_i = 0, \text{ con } k = 1, \ldots, r. \tag{5.11}$$

Sea $x \in L$ cualquiera. Entonces existen $\lambda_1, \ldots, \lambda_r \in K$ tales que

$$x = \sum_{k=1}^{r} \lambda_k w_k.$$

Multiplicando por λ_k la k-ésima ecuación de (5.11) y sumando todas las ecuaciones tenemos:

$$0 = \sum_{k=1}^{r} \lambda_k \sum_{i=1}^{n} \sigma_i(w_k)a_i = \sum_{i=1}^{n} a_i\sigma_i\Big(\sum_{k=1}^{r} \lambda_k w_k\Big) = \sum_{i=1}^{n} a_i\sigma_i(x),$$

lo cual contradice el teorema 5.7.12. En consecuencia, $|L : K| \geq n$.

Para demostrar que $|L : K| = n$ es suficiente verificar que cualquier conjunto con $n+1$ elementos de L es linealmente dependiente.

Sean $y_1, \ldots, y_{n+1} \in L$. Entonces, el sistema de ecuaciones lineales

$$\sum_{k=1}^{n+1} \sigma_i^{-1}(y_k)x_k = 0, \text{ con } i = 1, \ldots, n \tag{5.12}$$

admite una solución no trivial, digamos $(a_1, \ldots, a_{n+1}) \in L^{n+1}$ con $a_l \neq 0$. Nuevamente del teorema 5.7.12 se sigue que existe $k \in K$ tal que $T_U(k) \neq 0$. Definamos

$$x := (x_1, \ldots, x_{n+1}) := ka_l^{-1}(a_1, \ldots, a_{n+1}).$$

Es claro que x también es una solución del sistema (5.12) y, además, $x_l = k$. Por lo tanto, $T_U(x_l) \neq 0$. Aplicando σ_i sobre la i-ésima ecuación en (5.12) se tiene el sistema de ecuaciones

$$\sum_{k=1}^{n+1} y_k\sigma_i(x_k) = 0, \text{ con } i = 1, \ldots, n.$$

Sumando miembro a miembro todas las ecuaciones tenemos:

$$0 = \sum_{k=1}^{n+1} y_k \sum_{i=1}^{n} \sigma_i(x_k) = \sum_{k=1}^{n+1} y_k T_U(x_k) = \sum_{k=1}^{n+1} T_U(x_k)y_k.$$

Esto demuestra que se tiene una combinación no trivial del cero. Por lo tanto, el conjunto $\{y_1, \ldots, y_{n+1}\}$ es linealmente dependiente.

(3) Claramente $U \subseteq \mathrm{Aut}(L/K)$. Del teorema 5.6.23 se sigue que

$$|\mathrm{Aut}(L/K)| \leq |L : K| = n = |U|.$$

Por lo tanto, $\mathrm{Aut}(L/K) = U$.

(4) De (2) se tiene que L/K es una extensión finita y dado que

$$|\mathrm{Aut}(L/K)| = |L : K|,$$

del teorema 5.6.23 se sigue que L/K es separable. La normalidad se sigue del teorema 5.5.3. □

5.7.15 Definición. Sea L/K una extensión de cuerpos y $G := \mathrm{Aut}(L/K)$.

(1) Para $U \leq G$ definimos

$$\mathrm{Fix}(L, U) := \{x \in L \mid \sigma(x) = x, \ \forall \sigma \in U\}.$$

Dado que los elementos de G son K-automorfismos, se verifica que

$$K \subseteq \mathrm{Fix}(L,U) \subseteq L.$$

Es decir, $\mathrm{Fix}(L,U)$ es un cuerpo intermedio de L/K y lo llamamos `cuerpo fijo` de U sobre L.

(2) Si M es un cuerpo intermedio de L/K, entonces definimos

$$G_M := \{\sigma \in G \mid \sigma(x) = x,\ \forall x \in M\}.$$

Se verifica que $G_M \leq \mathrm{Aut}(L/K)$ y se denomina `grupo de isotropía` de M.

5.7.16 Ejemplo. (1) Sean $L = \mathbb{Q}(\sqrt{2},\sqrt{3})$ y $G := \mathrm{Aut}(L/\mathbb{Q})$. Estamos interesados en calcular $\mathrm{Fix}(L,G)$. Sabemos que

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \{(a+b\sqrt{2}) + (c+d\sqrt{2})\sqrt{3} \mid a,b,c,d \in \mathbb{Q}\}.$$

Sea $z = (a+b\sqrt{2}) + (c+d\sqrt{2})\sqrt{3} \in \mathrm{Fix}(L,G)$. Se tiene que

$$z = \sigma_2(z) = (a-b\sqrt{2}) + (c-d\sqrt{2})\sqrt{3}.$$

Por lo tanto

$$2b\sqrt{2} + 2d\sqrt{2}\sqrt{3} = 0.$$

Es decir,

$$z = a + c\sqrt{3}.$$

Por otro lado,

$$z = \sigma_1(z) = a - c\sqrt{3}.$$

Por consiguiente, $c = 0$ y se tiene que $z = a$. Es decir,

$$\mathrm{Fix}(L,G) = \mathbb{Q}.$$

(2) Sea $L = \mathbb{Q}(\sqrt[4]{2})$. Es claro que $L/\mathbb{Q}$ no es una extensión de Galois. Sea $\sigma \in G := \mathrm{Aut}(L)$ y $a := \sqrt[4]{2}$. Note que $m_{a,\mathbb{Q}} = x^4 - 2$ y debe cumplirse que $\sigma(a)$ sea también una raíz de $m_{a,\mathbb{Q}}$. Es decir,

$$\sigma(a) \in \{a, -a, a\mathrm{i}, -a\mathrm{i}\}.$$

Pero, la opciones complejas no son posibles ya que estas no pertenecen a L. Es decir,

$$\sigma(a) = \pm a.$$

En particular se cumple que

$$\sigma(\sqrt{2}) = \sigma(a^2) = \sigma(a)^2 = \sqrt{2}.$$

Por lo tanto, $\sqrt{2} \in \mathrm{Fix}(L,G)$. Esto demuestra que

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subseteq \mathrm{Fix}(L,G).$$

5.7.17 Teorema fundamental de la teoría de Galois. Sea L/K una extensión de Galois y $G := \mathrm{Gal}(L/K)$. Notemos con $\mathcal{M}$ al conjunto de todos los cuerpos intermedios de L/K. Es decir,

$$\mathcal{M} := \{M \mid K \subseteq M \subseteq L\}.$$

Notemos además con $\mathcal{U}$ el conjunto de todos los subgrupos de G. Esto es,

$$\mathcal{U} := \{U \mid U \leq G\}.$$

Para $U \in \mathcal{U}$ se verifica que $\mathrm{Fix}(U, L) \in \mathcal{M}$. Definamos entonces $\varphi : \mathcal{U} \longrightarrow \mathcal{M}$ de la siguiente manera:

$$\varphi(U) := \mathrm{Fix}(L, U).$$

Para $M \in \mathcal{M}$ se tiene que $G_M \in \mathcal{U}$. Definamos entonces $\psi : \mathcal{M} \longrightarrow \mathcal{U}$ así:

$$\psi(M) := G_M.$$

Entonces:

(1) Las funciones φ y ψ son biyecciones y una es la inversa de la otra. Es decir, existe una correspondencia biunívoca entre los cuerpos intermedios de la extensión L/K y los subgrupos del grupo $\mathrm{Gal}(L/K)$.

(2) Para todo $M \in \mathcal{M}$ se verifica que $|G_M| = |L : M|$ y G_M es el grupo de Galois de L/M. Es decir,

$$G_M = \mathrm{Gal}(L/M).$$

En particular $G_K = \mathrm{Gal}(L/K)$.

(3) Para todo $U \in \mathcal{U}$ se verifica que $|L : \mathrm{Fix}(L, U)| = |U|$. En particular, si $U = G$, entonces $\mathrm{Fix}(L, G) = K$.

(4) Si $M_1, M_2 \in \mathcal{M}$ con $M_1 \subseteq M_2$, entonces

$$G_{M_1} \supseteq G_{M_2}$$

y si $U_1, U_2 \in \mathcal{U}$ con $U_1 \subseteq U_2$, entonces

$$\mathrm{Fix}(L, U_1) \supseteq \mathrm{Fix}(L, U_2).$$

(5) Si $M \in \mathcal{M}$ y $\sigma \in G$, entonces

$$G_{\sigma(M)} = \sigma G_M \sigma^{-1}.$$

(6) Para $M \in \mathcal{M}$, la extensión M/K es de Galois si y solo si $G_M \trianglelefteq G$. Es decir,

$$G_M = \sigma G_M \sigma^{-1}, \quad \forall\ \sigma \in G.$$

Demostración.

(1) - (2) - (3) Sea $M \in \mathcal{M}$. Entonces, de la definición de G_M se sigue que $G_M = \mathrm{Aut}(L/M)$. Definamos

$$M' := \mathrm{Fix}(L, G_M).$$

Es claro que $M \subseteq M'$. De los teoremas 5.7.14 y 5.7.7 se sigue que

$$|L : M'| = |G_M| = |\mathrm{Aut}(L/M)| = |L : M|.$$

En consecuencia, $M' = M$. Esto demuestra que $\varphi(\psi(M)) = M$ para todo $M \in \mathcal{M}$. Es decir,

$$\varphi \circ \psi = I_{\mathcal{M}}.$$

Sea $U \in \mathcal{U}$ y definamos $M := \mathrm{Fix}(L, U)$. Del teorema 5.7.14 se sigue que

$$|L : M| = |U|$$

y que

$$U = \mathrm{Aut}(L/M) = G_M.$$

Esto prueba que $\psi(\varphi(U)) = U$ para todo $U \in \mathcal{U}$. Esto es,

$$\psi \circ \varphi = I_{\mathcal{U}}.$$

(4) Sean $M_1, M_2 \in \mathcal{M}$ con $M_1 \subseteq M_2$. Dado que todo automorfismo de L que deja fijo a M_2 también deja fijo a M_1, se sigue que

$$G_{M_1} \supseteq G_{M_2}.$$

Sean $U_1, U_2 \in \mathcal{U}$ con $U_1 \subseteq U_2$. Si un elemento de L es fijado por U_2, entonces también lo es por U_1. En consecuencia, se tiene la afirmación.

(5) Observe inicialmente que para $m \in M$ y $\mu \in G_M$ se verifica que

$$\sigma\mu\sigma^{-1}(\sigma(m)) = \sigma(m).$$

Es decir, cada elemento del cuerpo $\sigma(M)$ es fijado por $\sigma G_M \sigma^{-1}$. Esto trae como consecuencia que

$$\sigma G_M \sigma^{-1} \subseteq G_{\sigma(M)} = \mathrm{Aut}(L/\sigma(M)).$$

Por otro lado, dado que σ es biyectiva, se tiene que

$$|\sigma(M) : K| = |M : K|.$$

En consecuencia, $|L : \sigma(M)| = |L : M|$ y se sigue que

$$|\sigma G_M \sigma^{-1}| = |G_M| = |L : M| = |L : \sigma(M)| = |G_{\sigma(M)}|$$

y, por lo tanto, $G_{\sigma(M)} = \sigma G_M \sigma^{-1}$.

(6) Sea $M \in \mathcal{M}$. La separabilidad de M/K es inmediata. Por lo tanto, la extensión M/K es de Galois si y solo si M/K es una extensión normal. Como consecuencia del teorema 5.5.3 podemos afirmar que M/K es de Galois si y solo si $\sigma(M) = M$ para todo $\sigma \in G$. Por la parte (5) esta condición es equivalente a $\sigma G_M \sigma^{-1} = G_M$ para todo $\sigma \in G$. Es decir, M/K es una extensión de Galois si y solo si $G_M \trianglelefteq G$. □

5.7.18 Corolario. (1) Si L/K es un extensión finita separable, entonces L/K admite solo un número finito de cuerpos intermedios.

(2) Si L/K es un extensión de Galois con $\mathrm{Gal}(L/K)$ abeliano y si M es un cuerpo intermedio de L/K, entonces M/K también es una extensión de Galois.

Demostración.

(1) Para toda extensión algebraica L/K existe una extensión N/L tal que N/K es normal. (Se deja como ejercicio su prueba). Dado que L/K es separable, se puede obtener a N a partir de K adjuntando raíces de polinomios separables sobre K. Por lo tanto, N/K es separable y, en consecuencia, una extensión de Galois. Del teorema fundamental se sigue que N/K admite solo un número finito de cuerpos intermedios, lo cual también se cumple para L/K.

(2) En un grupo abeliano todos los subgrupos son normales. □

5.7.19 Ejemplo. Sean $a = \sqrt[3]{7}$ y ζ como en el ejemplo 5.4.8. Se demostró que $L := \mathbb{Q}(a, \zeta)$ satisface $|L : \mathbb{Q}| = 6$. Por lo tanto, $|\mathrm{Gal}(L/\mathbb{Q})| = 6$. Para determinar el grupo de Galois de $L/\mathbb{Q}$ es necesario conocer qué elementos de L son aplicados a y ζ. Para ello consideremos la siguiente tabla:

	a	ζ
σ_1	$a\zeta$	ζ
σ_2	a	ζ^2

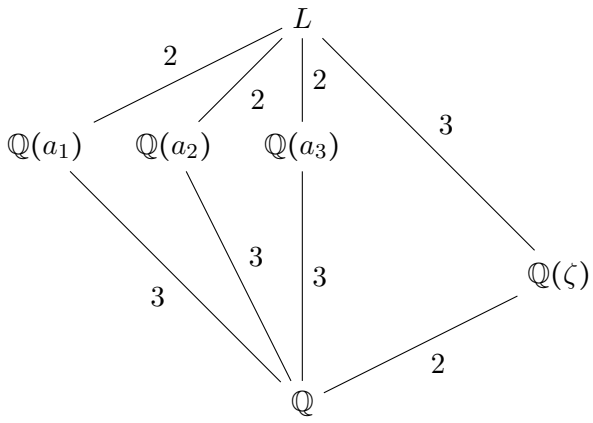
Note que $\sigma_1^3 = \sigma_2^2 = I_L$. Por lo tanto,

$$\mathrm{Gal}(L/\mathbb{Q}) = \{I_L, \sigma_1, \sigma_1^2, \sigma_2, \sigma_1\sigma_2, \sigma_1^2\sigma_2\}.$$

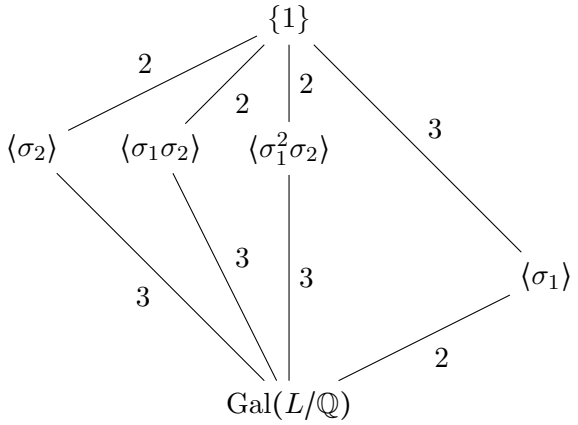
Los respectivos cuerpos intermedios están dados por

$$L,\ \mathbb{Q}(a),\ \mathbb{Q}(\zeta),\ \mathbb{Q}(a\zeta),\ \mathbb{Q}(a\zeta^2),\ \mathbb{Q}.$$

El retículo de los cuerpos intermedios es:



El retículo de los subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$ es:

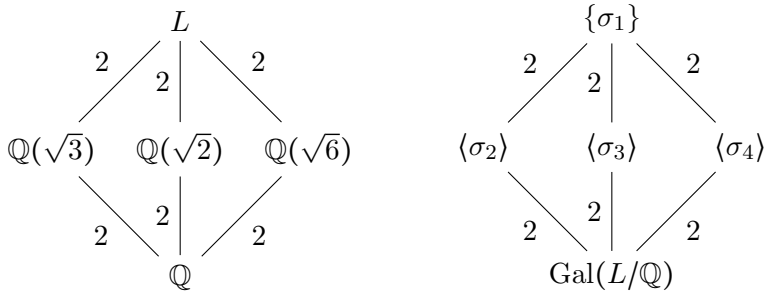


5.7.20 Ejemplo. En el ejemplo 5.7.10 se demostró que para $L = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ se verifica que $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo al 4-grupo de Klein.

Note que

$$\begin{aligned}
\mathrm{Fix}(L, \langle\sigma_1\rangle) &= L \\
\mathrm{Fix}(L, \langle\sigma_2\rangle) &= \mathbb{Q}(\sqrt{3}) \\
\mathrm{Fix}(L, \langle\sigma_3\rangle) &= \mathbb{Q}(\sqrt{2}) \\
\mathrm{Fix}(L, \langle\sigma_4\rangle) &= \mathbb{Q}(\sqrt{6}) \\
\mathrm{Fix}(L, G) &= \mathbb{Q}.
\end{aligned}$$

Los retículos de los subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$ y los cuerpos intermedios se presentan a continuación:



5.7.21 Ejemplo. Sea $f = x^5 - 1 \in \mathbb{Q}[x]$. Entonces,

$$f = (x-1)(x^4+x^3+x^2+x+1) = (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4),$$

donde ζ es una raíz quinta compleja de la unidad. El cuerpo de descomposición de f es $L := \mathbb{Q}(\zeta)$ y, en consecuencia, $|L:\mathbb{Q}| = 4$. Esto implica que $|\mathrm{Gal}(L/\mathbb{Q})| = 4$.

Cada $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ debe satisfacer que $\sigma(\zeta)$ es una raíz de f. Es decir, debe verificarse que

$$\sigma(\zeta)^4 + \sigma(\zeta)^3 + \sigma(\zeta)^2 + \sigma(\zeta) + 1 = \sigma(\underbrace{\zeta^4+\zeta^3+\zeta^2+\zeta+1}_{=0}) = 0.$$

Esta condición se satisface para cada σ_j definida como sigue

$$\begin{aligned}\sigma_1(\zeta) &:= \zeta^2\\ \sigma_2(\zeta) &:= \zeta^4\\ \sigma_3(\zeta) &:= \zeta^3\\ \sigma_4(\zeta) &:= \zeta.\end{aligned}$$

Se verifica sin dificultades que

$$\sigma_1^2 = \sigma_2,\ \sigma_1^3 = \sigma_3,\ \sigma_1^4 = \sigma_4.$$

Es decir,

$$\mathrm{Gal}(L/\mathbb{Q}) = \{I_L, \sigma_1,\ \sigma_1^2,\ \sigma_1^3\} = \langle\sigma_1\rangle \cong \mathbb{Z}_4.$$

El único subgrupo no trivial de G es $\langle\sigma_1^2\rangle = \{I_L,\ \sigma_1^2\}$.

Los cuerpos intermedios de $L/\mathbb{Q}$ son:

$$\begin{aligned}\mathrm{Fix}(L, \{I_L\}) &= L\\ \mathrm{Fix}(L, \langle\sigma_1^2\rangle) &= \mathbb{Q}(\zeta+\zeta^3)\\ \mathrm{Fix}(L, G) &= \mathbb{Q}.\end{aligned}$$

Los retículos de los subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$ y los cuerpos intermedios se presentan a continuación:

$$\begin{array}{ccc} L & & \{I_L\} \\ 2 \big| & & 2 \big| \\ \mathbb{Q}(\zeta+\zeta^3) & & \langle\sigma_1^2\rangle \\ 2 \big| & & 2 \big| \\ \mathbb{Q} & & \mathrm{Gal}(L/\mathbb{Q}) \end{array}$$

5.7.22 Ejemplo. Sea $f = x^4 - 2 \in \mathbb{Q}[x]$. Entonces,

$$f = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}\mathrm{i})(x + \sqrt[4]{2}\mathrm{i}).$$

El cuerpo de descomposición de f es $L := \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$ y se demostró en el ejemplo 5.5.4 (2) que $|L : \mathbb{Q}| = 8$. Por lo tanto, $|\mathrm{Gal}(L/\mathbb{Q})| = 8$.

Sea $G := \mathrm{Gal}(L/\mathbb{Q})$. Cada $\sigma \in G$ queda determinado por su acción sobre $\sqrt[4]{2}$ y sobre i. Se verifica que

$$\sigma(\mathrm{i}) \in \{\mathrm{i}, -\mathrm{i}\} \quad \text{y} \quad \sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2},\ -\sqrt[4]{2},\ -\sqrt[4]{2}\mathrm{i},\ \sqrt[4]{2}\mathrm{i}\}.$$

Definamos σ_1 y σ_2 de la siguiente manera:

	$\sqrt[4]{2}$	i
σ_1	$\sqrt[4]{2}\mathrm{i}$	i
σ_2	$\sqrt[4]{2}$	$-\mathrm{i}$

Entonces,

	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}\mathrm{i}$	$-\sqrt[4]{2}\mathrm{i}$
σ_1	$\sqrt[4]{2}\mathrm{i}$	$-\sqrt[4]{2}\mathrm{i}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}$
σ_2	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}\mathrm{i}$	$\sqrt[4]{2}\mathrm{i}$

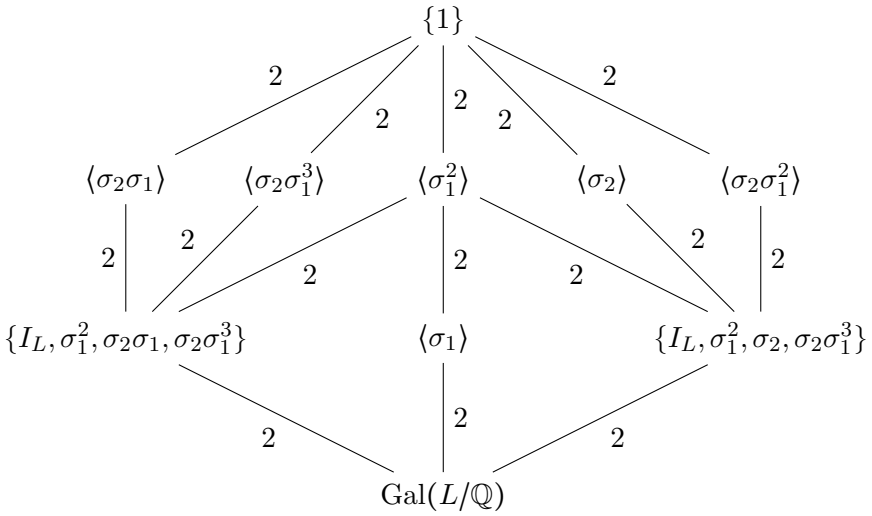
Se verifica sin dificultades que

$$\sigma_1^4 = \sigma_2^2 = I_L,\ \sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 = \sigma_1^{-1}$$

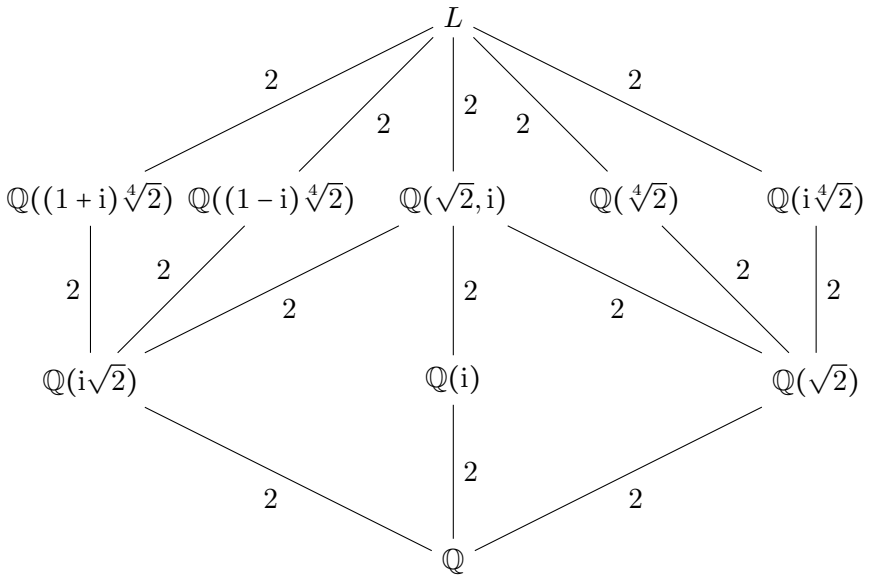
y que

$$G = \langle\sigma_1\rangle \cup \sigma_2\langle\sigma_1\rangle = \{I_l, \sigma_1, \sigma_1^2, \sigma_1^3, \sigma_2, \sigma_2\sigma_1, \sigma_2\sigma_1^2, \sigma_2\sigma_1^3\}.$$

Entonces, G es un grupo diédrico de orden 8. El retículo de los subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$ se presenta a continuación:



El teorema fundamental garantiza la existencia de 8 cuerpos intermedios no triviales, correspondientes a los cuerpos fijos de los subgrupos anteriores.



Como ilustración calculamos el cuerpo fijo del subgrupo $U := \langle \sigma_2 \rangle$. Es claro que U deja fijo a $\mathbb{Q}(\sqrt[4]{2})$. Por lo tanto, $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathrm{Fix}(L, U)$. Dado que $|L : \mathrm{Fix}(L, U)| = |U| = 2$ y $|L : \mathbb{Q}(\sqrt[4]{2})| = 2$ se sigue que

$$\mathrm{Fix}(L, U) = \mathbb{Q}(\sqrt[4]{2}).$$

5.7.23 Ejemplo. La extensión $\mathbb{R}/\mathbb{Q}$ no es algebraica. Por lo tanto, no es una extensión de Galois.

Note que para todo $\sigma \in \mathrm{Aut}(\mathbb{R})$ y todo $z \in \mathbb{Z} \setminus \{0\}$ se verifica

$$\sigma(z) = z\sigma(1) = z.$$

Dado que

$$1 = \sigma\left(\frac{z}{z}\right) = z\sigma\Big(\frac{1}{z}\Big)$$

para todo $z \in \mathbb{Z} \setminus \{0\}$ se verifica que

$$\sigma\Big(\frac{1}{z}\Big) = \frac{1}{z}.$$

Por lo tanto, para todo $z' \in \mathbb{Z}$ y todo $z \in \mathbb{Z} \setminus \{0\}$

$$\sigma\Big(\frac{z'}{z}\Big) = \frac{z'}{z}.$$

Si $\sigma \in \mathrm{Aut}(\mathbb{R})$ y $x > 0$, entonces existe $y \in \mathbb{R}$ tal que $y^2 = x$. Por consiguiente,

$$\sigma(x) = \sigma(y^2) = \sigma(y)^2 > 0.$$

Es decir, si $x \geq 0$, entonces $\sigma(x) \geq \sigma(0)$. Dado que σ es un homomorfismo si $x \geq y$, entonces $\sigma(x) \geq \sigma(y)$.

Sea $x \in \mathbb{R}$ y $\{x_k\}_{k\in\mathbb{N}} \subseteq \mathbb{Q}$ tal que

$$x_n \to x.$$

Entonces, para todo $\epsilon \in \mathbb{N}$ existe $N(\epsilon) \in \mathbb{N}$ tal que para todo $k \geq N(\epsilon)$

$$x - \frac{1}{\epsilon} \leq x_k \leq x + \frac{1}{\epsilon}.$$

En consecuencia,

$$\sigma(x) - \frac{1}{\epsilon} \leq x_k \leq \sigma(x) + \frac{1}{\epsilon},$$

con lo cual se tiene que

$$x_n \to \sigma(x).$$

La unicidad del límite implica que

$$\sigma(x) = x, \ \forall x \in \mathbb{R}.$$

Es decir,

$$\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{I_{\mathbb{R}}\}.$$

5.8 Ejercicios

(1) Se da un cuerpo K y un polinomio $f \in K[x]$. Determine en cada caso el cuerpo de descomposición L, así como el grado de la extensión $|L : K|$.

(a) $K = \mathbb{Q}$ y $f = x^p - 1$, con p un número primo.
(b) $K = \mathbb{Q}$ y $f = (x^2 - 3)(x^2 - 5)$.
(c) $K = \mathbb{Q}$ y $f = x^3 - 2$.
(d) $K = \mathbb{F}_2$ y $f = x^3 + x + 1$.
(e) $K = \mathbb{F}_2$ y $f = x^6 + 1$.
(f) $K = \mathbb{F}_2$ y $f = x^8 - x$.
(g) $K = \mathbb{F}_2$ y $f = x^4 + x^3 + x^2 + x + 1$.
(h) $K = \mathbb{F}_p$ y $f = x^{p^n} - 1$ con $n \in \mathbb{N}$ y p un número primo.

(2) ¿Cuántos elementos tiene el cuerpo de descomposición L del polinomio $f = x^{p^n} - x \in \mathbb{F}_p[x]$?

(3) Sea L el cuerpo de descomposición de un polinomio $f \in K[x]$ sobre el cuerpo K con $\operatorname{grad}(f) = n$. Demuestre que $|L : K| \mid n!$

(4) Sean $a := \sqrt{2} - \sqrt{3}$ y $b = \sqrt[3]{2} + i$. Determine $|\mathbb{Q}(a, b) : \mathbb{Q}|$.

(5) Determine $|\mathbb{Q}(i + \sqrt{2}) : \mathbb{Q}|$.

(6) Determine el grado de la extensión $\mathbb{Q}(\sqrt{2} + \sqrt{5})/\mathbb{Q}$.

(7) Determine el grado de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

(8) Determine, salvo isomorfía, todos los cuerpos con 2, 3, 4, 5, 8 y 9 elementos. Presente las tablas de adición y multiplicación en cada caso.

(9) Sea K un cuerpo con $\operatorname{Char}(K) \neq 2$. Sea $A \subseteq K^\times$ un conjunto finito con la siguiente propiedad:

(P) Para todo $\varnothing \neq M \subseteq A$ con M finito se verifica que

$$\prod_{m \in M} m$$

no es un cuadrado en K.

Demuestre que $|K(A) : K| = 2^{|A|}$ y que el sistema

$$\left(\sqrt{\prod_{m \in M} m} \;\middle|\; M \subseteq A \right)$$

es una base para $K(A)$ sobre K. Por convención, sea

$$\sqrt{\prod_{m\in\emptyset} m} = 1.$$

`Sugerencia:` inducción sobre $|A|$, defina

$$K_l := K(\sqrt{m_1}, \ldots, \sqrt{m_l})$$

y utilice el hecho que

$$K_{l+1} = K_l + \sqrt{a_{l+1}}K_l$$

`Corolario.` Sean $p_1, \ldots, p_n \in \mathbb{Z}$ números primos. Entonces,

$$|\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}| = 2^n. \tag{5.13}$$

(10) Sea $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ algebraico sobre $\mathbb{Q}$ con polinomio minimal $m_a \in \mathbb{Z}[x]$ de grado n.

(a) Demuestre que para todo $p/q \in \mathbb{Q}$ se verifica

$$\left| q^n f\left(\frac{p}{q}\right)\right| \geq 1.$$

(b) Con ayuda del teorema del valor medio demuestre que existe una constante $C_\alpha > 0$, tal que para todo $p/q \in \mathbb{Q}$ se verifica

$$\left|\alpha - \frac{p}{q}\right| > \frac{C_\alpha}{|q|^n}.$$

(c) Como consecuencia de lo anterior demuestre que el número

$$\sum_{k=1}^{\infty} 10^{-k!}$$

es trascendente sobre $\mathbb{Q}$.

(11) Para $a, b \in \mathbb{C}$ sean $\mathbb{Q}(a)/\mathbb{Q}$ y $\mathbb{Q}(b)/\mathbb{Q}$ extensiones de cuerpos cuadráticas con polinomios minimales $m_{a,\mathbb{Q}}$ y $m_{b,\mathbb{Q}}$ respectivamente.

(a) Sean $m_{a,\mathbb{Q}} = x^2 - 2$ y $m_{b,\mathbb{Q}} = x^2 - 4x + 2$. Halle un isomorfismo

$$\alpha : \mathbb{Q}(a) \longrightarrow \mathbb{Q}(b).$$

(b) Demuestre que $\mathbb{Q}(a) \cong \mathbb{Q}(b)$ si y solo si $\mathbb{Q}(a) = \mathbb{Q}(b)$.

(c) Muestre $a, b \in \mathbb{C}$ para los cuales $\mathbb{Q}(a) \ncong \mathbb{Q}(b)$.

(12) Sean L/K una extensión de cuerpos con $|L : K| = m$ y $f \in K[x]$ irreducible (sobre K) con $\text{grad}(f) = n$ y $\text{mcd}(m, n) = 1$. Demuestre que f es irreducible sobre L.

(13) Sean $\mathbb{F}_{p^n}$ y $\mathbb{F}_{p^m}$ cuerpos finitos con p^n y p^m elementos respectivamente. Demuestre que $\mathbb{F}_{p^n}$ es un subcuerpo de $\mathbb{F}_{p^m}$ si y solo si $n \mid m$.

(14) Describa la clausura algebraica de $\mathbb{F}_p$.

(15) Sean L/K una extensión de cuerpos y $f \in K[x]$ irreducible. Sean g, h factores irreducibles de f en $L[x]$. Demuestre que existe $\alpha \in \text{Aut}(L/K)$ tal que $\alpha(g) = h$.

(16) Sea K un cuerpo con $\text{Char}(K) \neq 2, 3$. Entonces son equivalentes:

(a) Toda suma de cuadrados en K es un cuadrado en K.

(b) Si un polinomio cúbico $f \in K[x]$ se descompone en factores lineales en $K[x]$, entonces f' también se descompone en factores lineales.

(17) En cada caso determine el grupo de Galois de K sobre $\mathbb{Q}$, así como el número de cuerpos intermedios M de $K/\mathbb{Q}$.

(a) $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$, donde cada $p_j \in \mathbb{Z}$ es un número primo con $p_i \neq p_j$ para $i \neq j$.

`Sugerencia:` tenga en cuenta (5.13) del ejercicio 9 y considere el efecto de multiplicar por $\sqrt{p_j}$ en K.

(b) $K = \mathbb{Q}(\sqrt{\zeta})$, donde $\zeta = e^{2\pi i/6}$.

(18) Sea $L \subseteq \mathbb{C}$ el cuerpo de descomposición del polinomio $f = x^5 - 2 \in \mathbb{Q}[x]$ y sea $\zeta = e^{2\pi i/5}$. Demuestre que

(a) $L = \mathbb{Q}(\sqrt[5]{2}, \zeta)$.

(b) $\text{Aut}(L/\mathbb{Q})$ es isomorfo al grupo $G \leq \text{Sym}(5)$ generado por los ciclos (12345) y (2354).

(c) Determine todos los subgrupos de G.

(d) Determine todos los cuerpos intermedios de $L/\mathbb{Q}$.

(e) ¿Para cuáles cuerpos intermedios M se verifica que la extensión $M/\mathbb{Q}$ es de Galois?

(19) Sea $K = \mathbb{F}_p$ y $L = K(x, y)$ el cuerpo de las funciones racionales en dos indeterminadas ($K(x, y) = Q(K[x, y])$). Considere $M = K(x^p, y^p)$. Demuestre que L/M es una extensión finita y que existen infinitos cuerpos intermedios entre M y L.

`Sugerencia:` considere $M(x + ty)$ con $t \in M$.

(20) Sea K un cuerpo y $L = K(x)$. Demuestre que:

$$\mathrm{Aut}(L/K) = \left\{ \alpha(x) = \frac{ax+b}{cx+d} \mid a,b,c,d \in K, \quad \text{y} \quad ad-bc \neq 0 \right\}.$$

(21) Sean K un cuerpo de característica cero y $L = K(x)$. Sean además $\sigma, \tau, \mu \in \mathrm{Aut}(L/K)$ definidas por

$$\sigma(x) = 1 - x$$
$$\tau(x) = -x$$
$$\mu(x) = \frac{1}{x}.$$

Demuestre que

(a) $|L : \mathrm{Fix}(L, \langle \sigma, \mu \rangle)| = 6$ y $\mathrm{Fix}(L, \langle \sigma, \mu \rangle) = K\left(\frac{(x^2-x+1)^3}{(x^2-x)^2}\right)$.

(b) El grupo $\langle \sigma, \tau \rangle$ es infinito y no abeliano.

(c) $K = \mathrm{Fix}(L, \langle \sigma, \tau \rangle) = \mathrm{Fix}(L, \langle \sigma\tau \rangle)$.

(d) $K(x^2) \cap K(x^2 - x) = K$.

(22) Sea K un cuerpo con $\mathrm{Char}(K) = p > 0$ y sea a un elemento algebraico sobre K. Entonces son equivalentes:

(a) $K(a)$ es separable sobre $K(a^p)$.

(b) $K(a) = K(a^p)$.

(c) $K(a)$ es separable sobre K.

(23) Sea L/K una extensión algebraica. Demuestre que

(a) Si K es perfecto, entonces L también lo es.

(b) Si L es perfecto, entonces no necesariamente K lo es.

(24) Demuestre que todo cuerpo algebraicamente cerrado es infinito.

(25) Demuestre que la extensión $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ es una extensión normal.

(26) Sea $K = \mathbb{Q}(\sqrt{7}, \sqrt{5})$. Determine $\mathrm{Aut}(K/\mathbb{Q})$ y establezca la correspondencia entre sus subgrupos y los cuerpos intermedios de la extensión $K/\mathbb{Q}$.

(27) Halle un elemento primitivo de $\mathbb{Q}(i, i\sqrt{2}, i\sqrt{3})$.

(28) Sea K un cuerpo con $\mathrm{Char}(K) = p > 0$. Sea L una extensión algebraica de K y defina

$$P := \{a \in L \mid a^{p^n} \in K \text{ para algún } n \in \mathbb{N}\}.$$

Demuestre que P es un cuerpo intermedio de la extensión L/K.

(29) Sea K un cuerpo finito con $|K| = q$. Demuestre que todo elemento de K es raíz del polinomio

$$f = x^q - x.$$

(30) Demuestre que el grupo multiplicativo de todo cuerpo finito es un grupo cíclico.

(31) Sean L y K cuerpos finitos con $|K| = q$ y $|L : K| = n$. Demuestre que $\mathrm{Aut}(L/K)$ es un grupo cíclico generado por el automorfismo de Frobenius.

(32) Sea K el cuerpo de descomposición de $f = x^6 + 1 \in \mathbb{Z}_2[x]$. Determine $\mathrm{Aut}(K/\mathbb{Z}_2)$.

(33) Sea $f = x^5 - 1 \in \mathbb{Q}[x]$. Determine:

(a) El cuerpo de descomposición de f, digamos L.

(b) $G \coloneqq \mathrm{Aut}(L/\mathbb{Q})$.

(c) Elabore el retículo de los cuerpos intermedios de L/K, así como el de los subgrupos de G.

(34) Sea $f = x^3 - 3 \in \mathbb{Q}[x]$.

(a) ¿Es f irreducible sobre $\mathbb{Q}$?

(b) Determine un cuerpo de descomposición L de f.

(c) Halle todos los cuerpos intermedios entre L y $\mathbb{Q}$.

(d) Determine el grupo $G \coloneqq \mathrm{Aut}(L/\mathbb{Q})$.

(e) Determine cuáles de las extensiones encontradas de $\mathbb{Q}$ son normales y cuáles son de Galois.

(35) Demuestre que la extensión $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es de Galois.

(36) Sea M un cuerpo intermedio de la extensión de Gaolois L/K. ¿Se verifica siempre que M/K es de Galois?

(37) Sea p un número entero primo, $m, n \in \mathbb{N}$ con $n > 0$ y $p \nmid m$. Demuestre que $\sqrt[n]{pm}$ no es un número racional.

(38) Sean $F = \mathbb{Z}_p$ y K una extensión de F con $|K : F| = 5$. Determine el grupo de Galois de la extensión.

(39) Sea $L \subseteq \mathbb{C}$ el cuerpo de descomposición del polinomio $f = x^5 - 2 \in \mathbb{Q}[x]$ y sea $\zeta = e^{2\pi i/5}$. Demuestre que

(a) $L = \mathbb{Q}(\sqrt[5]{2}, \zeta)$.

(b) $\mathrm{Aut}(L/\mathbb{Q})$ es isomorfo al grupo $G \leq \mathrm{Sym}(5)$ generado por los ciclos (12345) y (2354).

(c) Determine todos los subgrupos de G.

(d) Determine todos los cuerpos intermedios de $L/\mathbb{Q}$.

(e) ¿Para cuáles cuerpos intermedios M se verifica que la extensión $M/\mathbb{Q}$ es de Galois?

(40) Halle el cuerpo de descomposición K de $f = x^6 + 1 \in \mathbb{Z}_2[x]$ y determine $\mathrm{Aut}(K/\mathbb{Z}_2)$.

(41) Sean K un cuerpo finito con $\mathrm{char}(K) = p$ y $0 \neq a \in K$. Demuestre que para $m, n \in \mathbb{Z}$ se verifica que $ma = na$ si y solo si $m \equiv n \bmod p$.

(42) ¿Es $\mathbb{Q}(\sqrt{2})$ una extensión algebraica de $\mathbb{Q}$?

(43) Demuestre que la extensión $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es de Galois.

(44) Demuestre que toda extensión de grado 2 es normal.

(45) Sea M un cuerpo intermedio de la extensión de Galois L/K. Se verifica siempre que M/K es de Galois?

(46) Sea $f = x^4 - 1 \in \mathbb{Q}[x]$.

(a) Encuentre el cuerpo de descomposición L de f.

(b) Determine $\mathrm{Aut}(L/K)$.

(c) Elabore los retículos de los cuerpos intermedios y de L/K, así como de los subgrupos de $\mathrm{Aut}(L/K)$.

(47) Sea K un cuerpo finito. Demuestre que $(K^\times, \cdot)$ es un grupo cíclico. Como ilustración, determine un generador de $(\mathbb{Z}_7^\times, \cdot)$.

(48) Sea $a \in \mathbb{C}$ una raíz del polinomio $f = x^5 - 2x^4 + 6x + 10 \in \mathbb{Q}[x]$. Determine el polinomio minimal sobre $\mathbb{Q}$ de $a + r$ con $r \in \mathbb{Q}$.

(49) Sea L una extensión de un cuerpo K y $a_1, \ldots, a_n \in L$ con polinomios minimales $m_1, \ldots, m_n \in K[x]$ respectivamente. Demuestre que:

$$|K(a_1, \ldots, a_n) : K| \leq \prod_{i=1}^{n} \mathrm{grad}(m_i).$$

Considere el caso particular $K = \mathbb{Q}$ y $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$. ¿Se verifica la igualdad de la afirmación anterior?

(50) ¿Es $\mathbb{Q}(\sqrt{2})$ una extensión algebraica de $\mathbb{Q}$?

(51) Demuestre o refute:

(a) Todo cuerpo tiene extensiones no triviales.

(b) Todo cuerpo tiene extensiones algebraicas no triviales.

(c) Toda extensión simple es algebraica.

(d) Todas las extensiones algebraicas simples de un cuerpo K son isomorfas (como cuerpos).

(e) Toda extensión algebraica es simple.

CAPÍTULO 6

INTRODUCCIÓN A LOS CUERPOS FINITOS

La teoría de los cuerpos finitos es sin duda el punto inicial para la construcción de múltiples objetos combinatorios y geométricos. Algunas aplicaciones de estas construcciones pueden encontrarse por ejemplo en la teoría clásica de códigos, en la teoría de códigos de red o en la criptografía. Por fuera de las matemáticas, a finales del siglo XX se desarrollaron otras aplicaciones relacionadas con la informática y tecnología.

Desde un punto de vista histórico, la teoría de los cuerpos finitos se inició entre los siglos XVII y XVIII y el fundamento fue el estudio de cuerpos de clases residuales módulo un número primo y enfocado desde la óptica de la teoría de números. Algunos de los matemáticos involucrados fueron P. Fermat[1], L. Euler[2], J. L. Lagrange[3] y A. M. Legendre[4].

Los cuerpos finitos fueron tratados de manera general durante el siglo XIX, destacándose los trabajos cruciales de K. F. Gauss y E. Galois[5]. Algunos afirman que estos intercambiaron cartas con la demostración de la existencia de cuerpos finitos con orden la potencia de un número primo.

[1]Pierre de Fermat (Beaumont, Francia, 1601 - Castres, id., 1665) Matemático francés. Trabajó en el campo de los números enteros, probabilidad y geometría analítica.

[2]Leonhard Euler (Basilea, Suiza, 1707 - San Petersburgo, 1783) Matemático suizo. Uno de los más eminentes matemáticos de su tiempo.

[3]Joseph Louis de Lagrange (Turín, 1736 - París, 1813) Matemático francés de origen italiano. Estudió en su ciudad natal y hasta los diecisiete años no mostró ninguna aptitud especial para las matemáticas.

[4]Adrien-Marie Legendre (París, 1752-Auteuil, Francia, 1833) Matemático francés. A partir de 1795 enseñó matemáticas en la École Normale. En sus primeros trabajos introdujo conceptos como la función que lleva su nombre o la primera demostración del método de los mínimos cuadrados.

[5]Évariste Galois (Bourg-la-Reine, Francia, 1811 - París, 1832) Matemático francés. Estudió en el Collège Royal de Louis-le-Grand, donde enseguida mostró unas extraordinarias aptitudes para las matemáticas.

Una demostración precisa de este hecho se debe a R. Dedekind (1857) y a C. Jordan (1870). La unicidad de los cuerpos finitos fue demostrada por E. C. Moore en 1893. Es probable que la primera vez en que la teoría de cuerpos finitos fue presentada en forma de libro se deba a L.E. Dickson [4], un alumno de Moore.

6.1 Preliminares

6.1.1 Lema. Si K es un cuerpo finito con $\mathrm{char}(K) = p$, entonces $|K| = p^n$ para algún $n \in \mathbb{N}$.

Demostración. Sea F el cuerpo primo de K. Entonces, K es un espacio vectorial sobre F. Si $B = (v_1, \ldots, v_n)$ es una base para K sobre F, entonces todo $v \in K$ puede escribirse de manera única en la forma

$$v = \sum_{j=1}^{n} a_j v_j$$

con $a_j \in F$. Para cada $a_j \in F$ existen exactamente p opciones. Por lo tanto, existen p^n vectores distintos. Es decir, $|K| = p^n$. □

6.1.2 Teorema. Sea K un cuerpo, no necesariamente finito. Entonces, todo subgrupo finito del grupo multiplicativo $K^\times$ es cíclico.

Demostración. Sea $G \leq K^\times$ finito y definamos $n := \exp(G)$. Entonces, para todo $g \in G$ se verifica que $g^n = 1$. Es decir, todo elemento de G es raíz del polinomio $f = x^n - 1 \in K[x]$. Dado que f tiene a lo más n raíces distintas, se verifica que $|G| \leq n$.

Por otro lado, existe $g \in G$ con $\mathrm{ord}(g) = n$. En consecuencia, $|G| = n$ y se tiene que $G = \langle g \rangle$. □

6.1.3 Ejemplo. Sean $K = \mathbb{C}$, $n \in \mathbb{N}$ y denotemos con U_n el conjunto de las n-ésimas raíces complejas de la unidad. Esto es:

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

Claramente U_n es no vacío. Para $a, b \in U_n$ se tiene

$$(ab^{-1})^n = a^n (b^{-1})^n = a^n (b^n)^{-1} = 1.$$

En consecuencia, $(U_n, \cdot) \leq (\mathbb{C}^\times, \cdot)$. Del teorema anterior se sigue que U_n es un grupo cíclico.

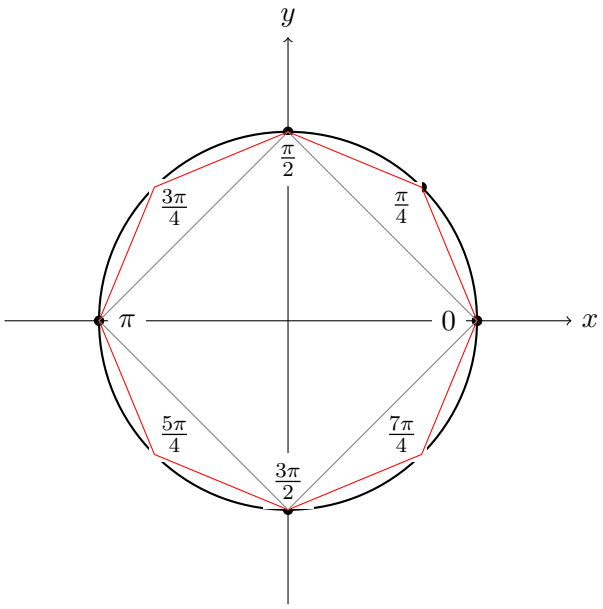
Para determinar un generador de U, sea $a \in \mathbb{C}^\times$ en forma polar, digamos $a = re^{i\varphi}$ con $r > 0$ y $0 \le \varphi < 2\pi$. Entonces,

$$\begin{aligned} a \in U_n &\Leftrightarrow r^n e^{in\varphi} = 1 \\ &\Leftrightarrow r^n = 1 \quad \wedge \quad e^{in\varphi} = 1 \\ &\Leftrightarrow r = 1 \quad \wedge \quad \varphi \in \{\tfrac{2k\pi}{n} \mid k = 0, 1, \ldots, n-1\}. \end{aligned}$$

Si definimos $\zeta_n := e^{i2\pi/n}$, entonces se tiene que

$$U_n = \{\zeta_n^k \mid k = 0, 1, \ldots, n-1\} = \langle \zeta_n \rangle.$$

Geométricamente podemos visualizar los elementos de U_n como los vértices de un polígono regular de n lados. Ilustramos a continuación los casos $n = 4$ y $n = 8$.



6.1.4 Teorema. Sea K un cuerpo finito con $|K| = q$. Entonces, todo elemento de K es raíz del polinomio $f = x^q - x$. Es decir para todo $a \in K$ se verifica que $a^q = a$.

Demostración. Sea $a \in K$. Si $a = 0$, entonces la afirmación es inmediata. Si $a \neq 0$, entonces

$$\operatorname{ord}(a) \mid |K^\times| = q - 1.$$

Por lo tanto,

$$a^q = a^{q-1}a = 1a = a.$$

Es decir para todo $a \in K$ se verifica que $a^q - a = 0$. $\square$

6.2 Existencia y unicidad de los cuerpos finitos

6.2.1 Teorema. Para toda potencia de un número primo $q = p^n$ existe, salvo isomorfía, un único cuerpo $\mathbb{F}_q$ con q elementos.

Demostración.

`Existencia.` Sean $f = x^q - x \in \mathbb{Z}_p[x]$ y K el cuerpo de descomposición de f. Sea además $A \subseteq K$ el conjunto de las raíces de f. Es decir,

$$A = \{a \in K \mid a^q = a\}.$$

Demostramos que $A = K$ y que $|K| = q$. Para todo $a \in \mathbb{Z}_p$ se verifica que $a^p = a$. Por lo tanto,

$$a^q = a^{p^n} = a^p = a.$$

Esto es, $\mathbb{Z}_p \subseteq A$.

Sean ahora $a, b \in A$ cualesquiera. Entonces,

$$(a-b)^q = (a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b,$$

y si $b \neq 0$

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}.$$

Esto demuestra que A es un subcuerpo de K que contiene a $\mathbb{Z}_p$. Dado que el cuerpo de descomposición de f es el cuerpo más pequeño que contiene a $\mathbb{Z}_p$ y a todas las raíces de f, se sigue que

$$\mathbb{Z}_p(A) = A = K.$$

Demostramos ahora que todo polinomio no constante que aparezca en la descomposición de f tiene multiplicidad 1. En efecto, note que

$$f' = p^n x^{p^n - 1} - 1 = -1.$$

Por lo tanto, del lema 5.6.6 se sigue que f no tiene raíces múltiples. En consecuencia, se tiene que $|A| = |K| = q$.

`Unicidad, salvo isomorfía.` Del teorema 6.1.4 se sigue que todo cuerpo L con q elementos es cuerpo de descomposición del polinomio $f = x^q - x$ sobre su subcuerpo primo. Dado que los cuerpos primos de K y L son isomorfos, se sigue que L y K también lo son. □

6.2.2 Ejemplos. (1) $\mathbb{F}_4$ es el cuerpo de descomposición de $f = x^4 - x$. Note que

$$f = x(x^3 - 1) = x(x-1)(x^2 + x + 1) \in \mathbb{Z}_2[x].$$

Los primeros dos factores nos dan las raíces 0 y 1. El polinomio $g = x^2 + x + 1$ es irreducible sobre $\mathbb{Z}_2$ y, en consecuencia, es el polinomio minimal de sus raíces. Sea $\omega \in \mathbb{F}_4$ una raíz de g. Entonces, dado que $|\mathbb{F}_4 : \mathbb{F}_2| = \text{grad}(g) = 2$ se tiene que

$$\mathbb{F}_4 = \mathbb{Z}_2(\omega) = \{x + y\omega \mid x, y \in \mathbb{Z}_2\} = \{0, 1, \omega, 1 + \omega\}.$$

Note que al ser ω una raíz de g se verifica que $\omega^2 = 1 + a$. Por lo tanto, si definimos $\beta := 1 + \omega$, las tablas de las operaciones en $\mathbb{F}_4$ son:

$+$	0	1	ω	β
0	0	1	ω	β
1	1	0	β	ω
ω	ω	β	0	1
β	β	ω	1	0

$\cdot$	0	1	ω	β
0	0	0	0	0
1	0	1	ω	β
ω	0	ω	β	1
β	0	b	1	ω

(2) $\mathbb{F}_8$ es el cuerpo de descomposición de $f = x^8 - x \in \mathbb{Z}_2[x]$. Se verifica que

$$f = x(x^7 - 1) = x(x - 1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

El polinomio $g = x^3 + x + 1$ es irreducible sobre $\mathbb{Z}_2$ y, en consecuencia, es el polinomio minimal de sus raíces. Sea $\omega \in \mathbb{F}_8$ una raíz de g. Entonces, dado que $|\mathbb{F}_8 : \mathbb{F}_2| = \text{grad}(g) = 3$ se tiene que

$$\begin{aligned}\mathbb{F}_8 &= \mathbb{Z}_2(\omega)\\ &= \{x + y\omega + z\omega^2 \mid x, y, z \in \mathbb{Z}_2\}\\ &= \{0, 1, \omega, \omega^2, 1 + \omega, 1 + \omega^2, \omega + \omega^2, 1 + \omega + \omega^2\}.\end{aligned}$$

(3) $\mathbb{F}_9$ es el cuerpo de descomposición de $f = x^9 - x \in \mathbb{Z}_3[x]$. Note que

$$f = x(x^8 - 1) = x(x - 1)(x + 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1).$$

El cuerpo primo de $\mathbb{F}_9$ es $\mathbb{Z}_3$. Por lo tanto, $\{0, 1, 2\} \subseteq \mathbb{F}_9$. Por otro lado, los polinomios $x^2 + 1$, $x^2 + x - 1$ y $x^2 - x - 1$ son irreducibles sobre $\mathbb{Z}_3$. Sea $\omega \in \mathbb{F}_9$ una raíz de $x^2 + 1$. Dado que $\mathbb{F}_9$ es una extensión cuadrádica de $\mathbb{Z}_3$, se tiene que

$$\begin{aligned}\mathbb{F}_9 &= \mathbb{Z}_3(\omega)\\ &= \{x + y\omega \mid x, y \in \mathbb{Z}_3\}\\ &= \{0, 1, 2, \omega, 2\omega, 1 + \omega, 1 + 2\omega, 2 + \omega, 2 + 2\omega\}.\end{aligned}$$

6.2.3 Lema. Sean $m, n \in \mathbb{N}$ y K un cuerpo. Entonces,

(1) $(x^m - 1) \mid (x^n - 1)$ en $K[x]$ si y solo si $m \mid n$ en $\mathbb{Z}$.

(2) $(p^m - 1) \mid (p^n - 1)$ en $\mathbb{Z}$ si y solo si $m \mid n$ en $\mathbb{Z}$.

DEMOSTRACIÓN. (1) Usando la división con resto se tiene que $n = sm + t$ con $s, t \in \mathbb{N}_0$ y $0 \leq t < m$ y, además,

$$\begin{aligned} x^n - 1 &= x^{sm+t} - 1 \\ &= x^t(x^{sm} - 1) + (x^t - 1) \\ &= x^t((x^m)^s - 1) + (x^t - 1) \\ &= x^t(x^m - 1)\sum_{j=0}^{s-1} x^{jm} + (x^t - 1). \end{aligned}$$

En consecuencia,

$$\begin{aligned} m \mid n &\Leftrightarrow t = 0 \\ &\Leftrightarrow x^t = 1 \\ &\Leftrightarrow (x^m - 1) \mid (x^n - 1). \end{aligned}$$

(2) Similar como (1). □

En el siguiente lema se demuestra que existe una correspondencia entre el retículo de los subcuerpos de $\mathbb{F}_{p^n}$ y el retículo de los divisores del número natural n.

6.2.4 Lema. Sean $m, n \in \mathbb{N}$ y $L \cong \mathbb{F}_{p^n}$. Entonces, L admite un subcuerpo $K \cong \mathbb{F}_{p^m}$ si y solo si $m \mid n$ en $\mathbb{Z}$.

DEMOSTRACIÓN. Supongamos que L admite un subcuerpo $K \cong \mathbb{F}_{p^m}$ y sea $d := |L : K|$. Entonces,

$$p^n = |L| = |K|^d = p^{md}.$$

En consecuencia, $m \mid n$.

Recíprocamente, supongamos que $m \mid n$ y denotemos con P el cuerpo primo de L. Del lema anterior se sigue que $(p^m - 1) \mid (p^n - 1)$ en $\mathbb{Z}$ y

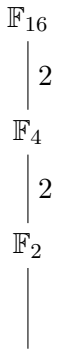
$$(x^{p^m-1} - 1) \mid (x^{p^n-1} - 1).$$

Note que L es un cuerpo de descomposición de $f := x^{p^n-1} - 1$ sobre P. Por lo tanto, L contiene un cuerpo de descomposición K de $f := x^{p^m-1} - 1$ sobre P. Claramente se verifica que $K \cong \mathbb{F}_{p^m}$. □

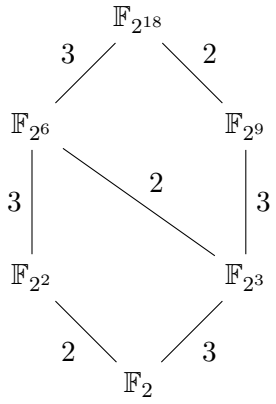
6.2.5 Ejemplos. (1) Los únicos subcuerpos de $\mathbb{F}_4$ son $\mathbb{F}_2$, que es su subcuerpo primo y $\mathbb{F}_4$.

(2) Los únicos subcuerpos de $\mathbb{F}_8$ son $\mathbb{F}_2$, que es su subcuerpo primo y $\mathbb{F}_8$.

(3) Los únicos subcuerpos de $\mathbb{F}_{16}$ son $\mathbb{F}_2$, $\mathbb{F}_4$ y $\mathbb{F}_{16}$. Una ilustración del retículo de subcuerpos de $\mathbb{F}_{16}$ es la siguiente:



(4) Los únicos subcuerpos de $\mathbb{F}_{2^{18}}$ son $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^9}$ y $\mathbb{F}_{2^{18}}$. Una ilustración del retículo de subcuerpos de $\mathbb{F}_{2^{18}}$ es la siguiente:



6.3 Extensiones de cuerpos finitos y automorfismos

6.3.1 Teorema. Toda extensión finita de un cuerpo finito es una extensión de Galois. Es decir, normal y separable.

Demostración. Sea K un cuerpo finito. Entonces, K es perfecto y cualquier extensión L/K es separable. Por otro lado, dado que L es cuerpo de descomposición de un polinomio de la forma $f = x^q - x$ para algún $q \in \mathbb{N}$, se tiene que L/K es normal. □

6.3.2 Teorema. Sea K un cuerpo finito, $|K| = q$ y L una extensión de K con $|L : K| = n$. Entonces, $\mathrm{Aut}(L/K)$ es un grupo cíclico de orden n y, además, $\varphi : L \longrightarrow L$ definida por $\varphi(x) = x^q$ genera a $\mathrm{Aut}(L/K)$.

DEMOSTRACIÓN. Del lema 5.1.6 se sigue que $\varphi \in \mathrm{Aut}(L)$.

Demostramos que $\varphi|_K = I_K$. Del teorema 6.1.4 se tiene que todo $a \in K$ es raíz de $f = x^q - x$. Es decir, para todo $a \in K$

$$0 = f(a) = a^q - a.$$

Por lo tanto, para todo $x \in K$ se verifica que $\varphi(x) = x$. Se sigue además que $\varphi \in \mathrm{Aut}(L/K)$.

Demostramos que $\varphi^n = I_L$. Dado que $|L| = q^n$, nuevamente del teorema 6.1.4 se sigue que para todo $x \in L$

$$\varphi^n(x) = x^{q^n} = x.$$

Demostramos que φ tiene orden n. Si $\mathrm{ord}(\varphi) = m < n$, entonces $\varphi^m = I_L$. Es decir, $a^{q^m} = a$ para todo $a \in L$. En consecuencia, todo $x \in L$ sería raíz del polinomio $f = x^{q^m} - x$, lo cual no es posible ya que $\mathrm{grad}(f) = q^m < q^n$.

Demostramos que $|\mathrm{Aut}(L/K)| \leq n$. Sea a un generador del grupo multiplicativo $L^\times$ de L. Entonces,

$$m_{a,K} = \sum_i k_i x^i.$$

Dado que

$$K[x]/(m_{a,K}) \cong K(a) = L,$$

se sigue que $\mathrm{grad}(m_{a,K}) = n$.

Para todo $\sigma \in \mathrm{Aut}(L/K)$ se verifica que $\sigma(a)$ es una raíz de $m_{a,K}$. En efecto,

$$0 = \sigma(m_{a,K}(a)) = \sum_{i=0}^{n} \sigma(k_i)\sigma(a)^i = \sum_{i=0}^{n} k_i \sigma(a)^i.$$

Dado que σ está determinado de manera única por $\sigma(a)$, se sigue que $|G| \leq n$. Esto demuestra que $|G| = n$ y que $G = \langle\varphi\rangle$. □

6.3.3 Corolario. $\mathrm{Aut}(\mathbb{F}_{p^n})$ es un grupo cíclico de orden n generado por el automorfismo de Frobenius $\varphi(x) = x^p$.

DEMOSTRACIÓN. Es una consecuencia inmediata del teorema anterior. Es suficiente tomar $K = \mathbb{F}_p$ y $L = \mathbb{F}_{p^n}$. □

6.3.4 Ejemplo. Grupos de automorfismos de cuerpos finitos binarios.

Cuerpo	Grupo de automorfismos	Tipo de isomorfía
$\mathbb{F}_4$	$\{\sigma_j \mid \sigma_j(x) = x^{2^j},\ \ j = 1, 2\}$	$\mathbb{Z}_2$
$\mathbb{F}_8$	$\{\sigma_j \mid \sigma_j(x) = x^{2^j},\ \ j = 1, 2, 3\}$	$\mathbb{Z}_3$
$\mathbb{F}_{16}$	$\{\sigma_j \mid \sigma_j(x) = x^{2^j},\ \ j = 1, 2, 3, 4\}$	$\mathbb{Z}_4$
$\mathbb{F}_{32}$	$\{\sigma_j \mid \sigma_j(x) = x^{2^j},\ \ j = 1, 2, 3, 4, 5\}$	$\mathbb{Z}_5$
$\vdots$		$\vdots$

6.3.5 Teorema fundamental de la teoría de Galois. Sea L/K una extensión de cuerpos, $|K| = q$ y $|L : K| = n$. Si $G = \mathrm{Aut}(L/K)$, entonces:

(1) La función

$$U \mapsto \mathrm{Fix}(L, U) \tag{6.1}$$

es una biyección entre el conjunto de los subgrupos de G y los cuerpos intermedios de L/K.

(2) La función

$$M \mapsto G_M \tag{6.2}$$

es la inversa de la función definida en (6.1). Además se verifica que

$$|U| = |L : \mathrm{Fix}(L, U)|.$$

En particular se tiene que $\mathrm{Fix}(L, G) = K$.

Demostración. Es claro que $L \cong \mathbb{F}_{q^n}$. Sea además φ el automorfismo de Frobenius de L sobre K. Dado que $G = \langle\varphi\rangle$ para todo $U \leq G$ se tiene que existe $m \in \mathbb{N}$ con $m \mid n$ tal que $U = \langle\varphi^m\rangle$.

Se verifica que

$$\begin{aligned}\mathrm{Fix}(L, U) &= \{a \in L \mid \sigma(a) = a,\ \ \forall\sigma \in U\}\\ &= \{a \in L \mid \varphi^m(a) = a\}\\ &= \{a \in L \mid a^{q^m} = a\}.\end{aligned}$$

Entonces, $\mathrm{Fix}(L, U)$ es el cuerpo de descomposición de $f = x^{q^m} - x$ y, en consecuencia,

$$\mathrm{Fix}(L, U) \cong \mathbb{F}_{q^m}.$$

Sea $M := \mathrm{Fix}(L, U)$. Demostramos que $G_M = U$. Claramente $U \subseteq G_M$.

Recíprocamente, sea $I_L \neq \varphi^s \in G_M$. Es decir,

$$\varphi^s(a) = a \ \text{ para todo } \ a \in M.$$

O equivalentemente,

$$a^{q^s-1} = 1 \quad \text{para todo} \quad 0 \neq a \in M.$$

Dado que $M^\times \cong \mathbb{F}_{q^m}^\times$ y este es cíclico de orden $q^m - 1$, se tiene que

$$q^m - 1 \mid q^s - 1.$$

Del lema 6.2.3 se sigue que $m \mid s$. Por lo tanto,

$$\varphi^s = \varphi^{mk} = (\varphi^m)^k$$

para algún $k \in \mathbb{N}$. En consecuencia, $\varphi^s \in U$ y se tiene que $G_M \subseteq U$.

Finalmente, usando resultados de la teoría de grupos tenemos:

$$\begin{aligned} |U| &= \operatorname{ord}(\varphi^m) \\ &= \frac{\operatorname{ord}(\varphi)}{\operatorname{mcd}(m, \operatorname{ord}(\varphi))} \\ &= \frac{n}{m} \\ &= \frac{|L:K|}{|\operatorname{Fix}(L,U):K|} \\ &= |L : \operatorname{Fix}(L,U)|, \end{aligned}$$

con lo cual se tiene la afirmación. □

CAPÍTULO 7

CONSTRUCCIÓN CON REGLA Y COMPÁS

7.1 Introducción

Los matemáticos de la antigua Grecia abordaron tres problemas que jugaron un papel importante en el desarrollo de la geometría clásica. Estos problemas consistían en duplicar el cubo, encontrar la cuadratura del círculo y trisecar un ángulo.

`La duplicación del cubo.` Existen dos versiones distintas sobre el origen de este problema. La primera afirma que Eratóstenes, en su obra *Platonicus*; relata que, alrededor del año 429 a. C. una peste asolaba a Atenas y el dios anunció por medio del oráculo de Apolos a los habitantes que, para deshacerse de la plaga, se debía construir un altar del doble del que había. Fueron muchos los esfuerzos por resolver el problema, de hacer un sólido que fuera el doble de otro sólido similar; no obtante, este permaneció sin resolver. La fábula sigue relatando que, al ser Platón interrogado sobre el probelma, este respondió que el oráculo no quiso decir que el dios deseaba un altar del doble del tamaño, sino que quería avergonzar a los griegos por su desprecio hacia la geometría. En total, la peste desapareció, pero el problema permaneció por varios siglos.

La segunda versión del problema, un poco diferente, se debe a un comentario de Eutocio al tratado de Arquímedes titulado *Sobre la esfera y el cilindro*. Esta versión se supone que es una carta escrita por Eratóstenes al rey Ptolomeo, que dice así: *La anécdota dice que uno de los poetas trágicos antiguos representaba a Minos haciendo construir una tumba para Glauco y que, cuando Minos descubrió que la tumba medía cien pies de cada lado, dijo "Demasiado pequeña es la tumba que habéis señalado como el sitio real de descanso. Hacedla el doble de grande. Sin arruinar la forma, rápidamente duplicad cada lado de la*

tumba". Esto evidentemente no presentaba una solución al problema. En efecto, si los lados del cubo se duplican, entonces su volumen se octuplica. Este relato no es más que un episodio de la mitología griega, no obstante, los descubrimientos en Cnosos, en Creta, en tiempos relativamente recientes han mostrado que, aunque parcialmente, estas fábulas están basadas en hechos históricos. La mitología relata que Glauco, el hijo de Minos, el rey de Creta y de su esposa Pasifae, murió siendo niño al caer en un recipiente de miel.

`La cuadratura del círculo.` Consiste en determinar si es posible, utilizando solo regla y compás, construir un cuadrado que tenga exactamente la misma área que un círculo dado. Este es probablemente el problema clásico más conocido. Arquímides fue el matemático de la antiguedad que presentó la más importante contribución. Este escribió un tratado sobre la medida del círculo, en el cual presenta un método para determinar el valor del número π con el grado de aproximación que se desee. Este método prevaleció hasta el siglo XVII. Los griegos no conocieron que para la solución geométrica de este problema, era necesario calcular con métodos geométricos el valor de la raíz cuadrada del número π. Siglos más tarde el matemático alemán K. Lindemann demostró que π es trascendente y, en consecuencia, el problema no podía ser resuelto solo con regla y compás.

`La trisección del ángulo.` La trisección del ángulo fue el tercero de los problemas clásicos de la antigua Grecia. Este consiste en dividir un ángulo dado en tres partes iguales. En general, este problema tampoco es soluble utilizando solo regla y compás. Una de las formas de ataque del problema fue la introducción de ciertas curvas auxiliares, por ejemplo, la famosa trisectriz de Hipias. Este nombre debido a su autor, el sofista Hipia de Elis. El matemático francés Pierre Wantzel demostró que un ángulo α es trisecable con regla y compás si el polinomio $f = 4x^3 - 3x - \cos(\alpha)$ es reducible.

7.2 Elementos construibles

A partir de $M \subseteq \mathbb{R}^2$ construiremos con regla y compás nuevos puntos del plano. Usaremos en adelante la siguiente notación:

- $P(L, L')$ denota el conjunto de todos los puntos que son intersección de dos rectas no paralelas L y L' que pasan por dos puntos distintos de M. (Ver figura 7.1).
- $P(L, k)$ es el conjunto de todos los puntos que son intersección de una recta que pasa por dos puntos distintos de M con una circunferencia con centro en un punto de M y radio k, siendo k la distancia entre dos puntos distintos de M. (Ver figura 7.2).
- $P(k, k')$ denota el conjunto de todos los puntos que son intersección de dos circunferencias que tienen centros en puntos distintos de M y cuyos radios k y k' son la distancia entre dos puntos distintos de M. (Ver figura 7.3).

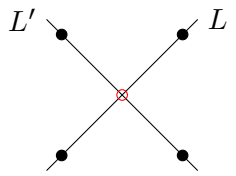


Figura 7.1: Intersección de dos rectas no paralelas.

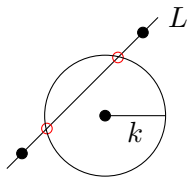


Figura 7.2: Intersección de una recta con una circunferencia.

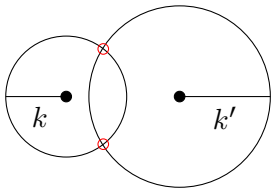


Figura 7.3: Intersección de dos circunferencias.

7.2.1 Definición. Sea $M \subseteq \mathbb{R}^2$. Definimos el conjunto M^+ de la siguiente manera:

$$M^+ := M \cup P(L, L') \cup P(L, k) \cup P(k, k'). \tag{7.1}$$

7.2.2 Ejemplos. Sea $M \subseteq \mathbb{R}^2$.

(1) Si $|M| \leq 1$, entonces $M^+ = M$.

(2) Si $M = \mathbb{R}^2$, entonces $M^+ = M$.

(3) Si $|M| = 2$, entonces $|M^+| = 6$. En efecto, $|P(L, k)| = |P(k, k')| = 2$.

Ilustración:

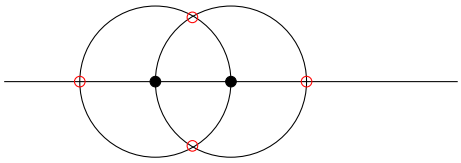


Figura 7.4: Un ejemplo del conjunto M^+.

7.2.3 Definición. Sea $M \subseteq \mathbb{R}^2$ con $|M| \geq 2$. Definimos recursivamente

$$M_0 := M$$
$$M_{n+1} := M_n^+ \quad \text{para } n \in \mathbb{N}_0.$$

En particular, se cumple que

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq M_{n+1} \subseteq \cdots$$

Llamaremos a

$$C(M) := \bigcup_{j \in \mathbb{N}_0} M_j$$

el conjunto de los `puntos construibles con regla y compás` a partir de M.

7.2.4 Ejemplo. (`Perpendicular a una recta`) Sean P, Q, R puntos dados. Para construir con regla y compás una recta que pase por R y que sea perpendicular a la recta L que pasa por los puntos P y Q. Procedemos de la siguiente manera:

- Se traza la circunferencia con centro en P que pasa por R.
- Se traza la circunferencia con centro en Q que pasa por R.
- Se traza la recta que une el punto R con el segundo punto de corte de las dos circunferencias. Esta recta es perpendicular a L. (Ver figura 7.5).

7.2.5 Ejemplo. (`Paralela a una recta`) Sean P, Q, R puntos dados. Para construir una recta que pase por R y sea paralela a la recta L que pasa por P y Q procedemos así:

- Se traza la circunferencia con centro en R y radio la distancia entre P y Q.
- Se traza la circunferencia con centro en Q y radio la distancia entre P y R.

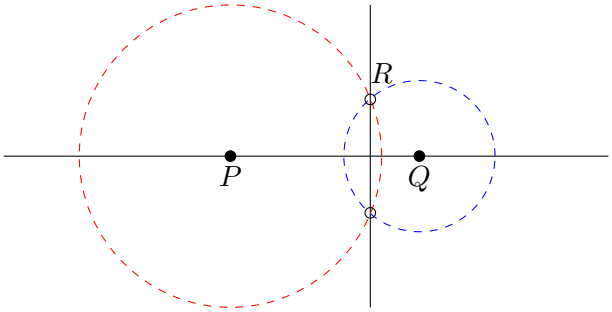


Figura 7.5: Perpendicular a una recta.

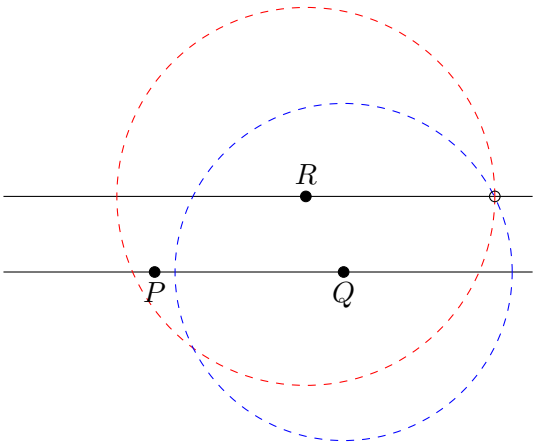


Figura 7.6: Paralela a una recta.

- Se traza adecuadamente la recta que une el punto R con uno de los puntos de corte de las circunferencias. Esta recta es paralela a L. (Ver figura 7.6).

7.2.6 Ejemplo. (`Mediatriz y punto medio de un segmento`) Sean P, Q, R puntos dados. Para construir la mediatriz del segmento que une a P y Q procedemos de la siguiente manera:

- Se trazan respectivamente las circunferencias con centro en P y Q con radios la distancia entre P y Q.

- La recta que une los puntos de corte de las dos circunferencias es la mediatriz del segmento.

Dados los puntos P y Q, trazamos el segmento de recta que los une. Luego se construye la mediatriz del segmento. El punto de intersección de esta con el segmento es el punto medio buscado. (Ver figura 7.7).

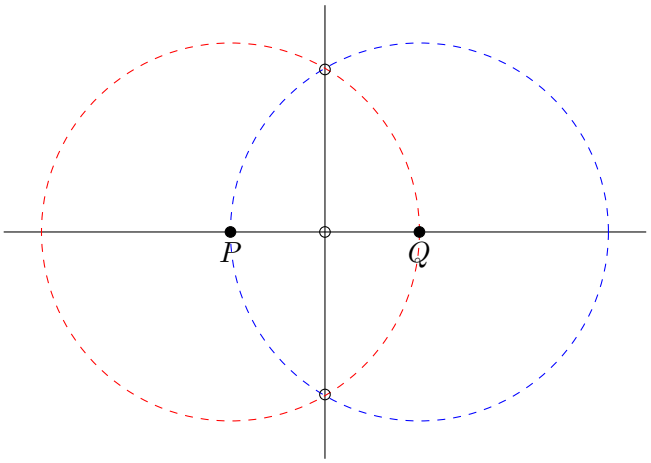


Figura 7.7: Mediatriz y punto medio de un segmento.

7.2.7 Ejemplo. (`Construcción de cualquier distancia entera`) Sean P, Q, R puntos dados. Se traza la recta que une los puntos P y Q y se toma como unidad la distancia entre P y Q, haciendo centro en Q trazamos una circunferencia de radio 1 y obtenemos otro punto al intersectar la circunferencia con la recta. Continuando con este proceso podemos obtener cualquier distancia entera.

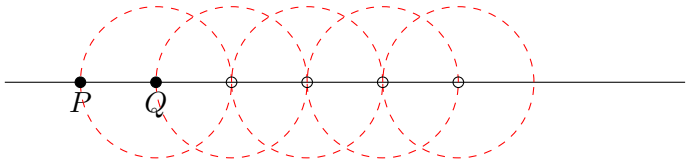


Figura 7.8: Distancias enteras.

7.2.8 Ejemplo. (`Bisectriz de un ángulo`) Sean P, Q, R puntos dados. Para bisecar el ángulo determinado por los puntos no colineales P, Q y R se procede de la siguiente manera:

- Se trazan las rectas L_1 y L_2 que pasan por P y Q y por P y R, respectivamente.

- Se traza la circunferencia con centro en P y radio la distancia entre P y Q. Esta circunferencia intersecta a L_2 en un punto T.
- Se trazan respectivamente las circunferencias con centros en T y Q, cuyos radios son la distancia entre T y Q.
- Se traza la recta que pasa por P y uno de los puntos de corte de estas circunferencias. Esta recta es la bisectriz del ángulo.

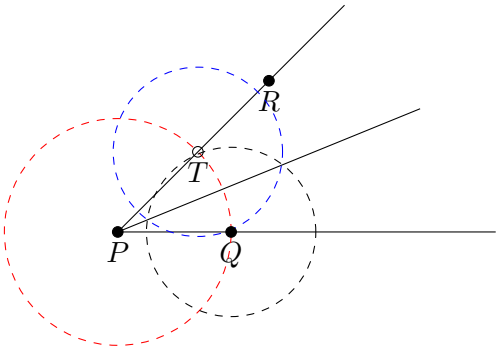


Figura 7.9: Bisectriz de un ángulo.

7.2.9 Ejemplo. (`División de un segmento en` n `partes iguales`) Sean P, Q, R puntos dados. Para obtener tal división, procedemos de la siguiente manera:

- Se traza el segmento que une los puntos $P_0 = P$ y $P_1 = Q$.
- Se traza la circunferencia con centro en cada uno de esos puntos y radio la distancia entre ellos y se obtienen dos puntos de corte de estas.
- Se toma uno de estos puntos de corte, digamos P_2 y trazamos la semirrecta que une a P con P_2. Llamemos a esta semirrecta L.
- Se traza la circunferencia con centro en P_2 y radio la distancia entre P_0 y P_2. Esta circunferencia corta a L en otro punto, digamos P_3.
- Se traza la circunferencia con centro en P_3 y radio la distancia entre P_0 y P_2. Esta circunferencia corta a L en otro punto, digamos P_4.
- Se continúa iteradamente con el proceso hasta que se haya dividido la semirrecta L en n partes iguales. Según nuestra notación, el proceso se detiene en el punto P_{n+1}.

- Se traza el segmento que une P_{n+1} con P_1 y seguidamente se trazan rectas paralelas a este que pasen por cada uno de los puntos obtenidos en la semirrecta L y que corten al segmento inicial.

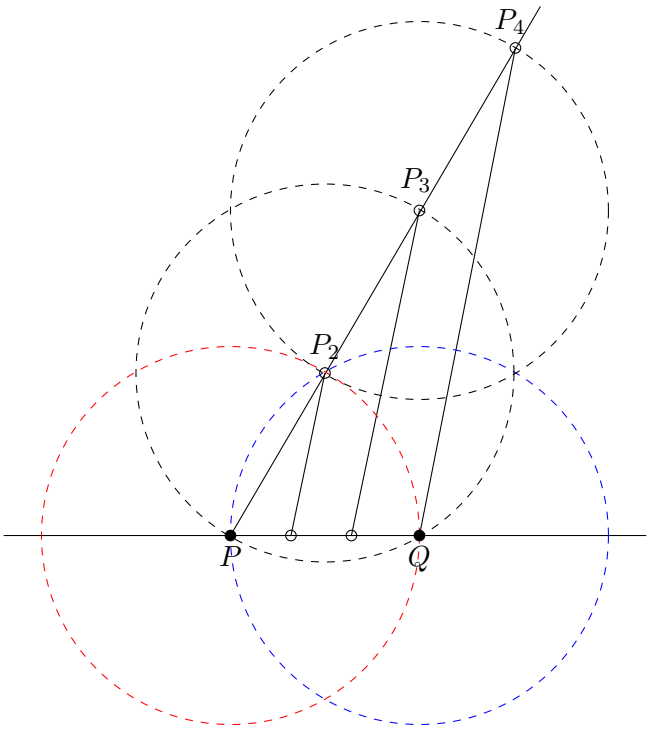


Figura 7.10: División de un segmento.

7.3 Estructura de cuerpo de $C(M)$

Para obtener una descripción algebraica del conjunto $C(M)$ presentamos inicialmente algunas construcciones importantes.

7.3.1 Ejemplo. (`Construcción de un sistema rectangular de coordenadas`) A partir de dos puntos P y Q se traza la recta que pasa por ellos y lo llamamos eje x. Luego se traza la mediatriz del segmento que los une y posteriormente se traza una paralela a esa mediatriz que pase por P, la cual llamaremos eje y. Obtenemos así unos ejes coordenados cuyo origen es P y cuya unidad de medida es la distancia entre P y Q. Podemos asociar entonces a los puntos P y Q los elementos $(0,0)$ y $(1,0)$ respectivamente. (Ver figura 7.11).

7.3.2 Ejemplo. (`Construcción del simétrico de un punto con respecto a otro`) Dados dos puntos P y Q se traza la recta que pasa por ellos. Seguidamente hacemos centro en P y trazamos la circunferencia con radio la distancia entre P y Q. Esta circunferencia corta a la recta anterior en otro punto que es exactamente el simétrico de Q con respecto de P. (Ver figura 7.12).

7.3.3 Ejemplo. (`Construcción de proyecciones de un punto sobre los ejes`) Sea $Q = (x, y)$ un punto construible. Si Q está sobre alguno de los ejes, entonces la proyección de este es él mismo. Supongamos entonces que Q no esté sobre algún eje. Entonces se trazan rectas paralelas a los ejes que pasan por P y obtenemos las proyecciones de Q sobre los ejes coordenados. Estos son $(x, 0)$ y $(0, y)$. (Ver figura 7.12).

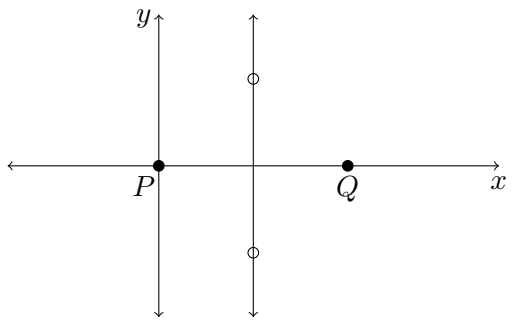


Figura 7.11: Sistema rectangular de coordenadas.

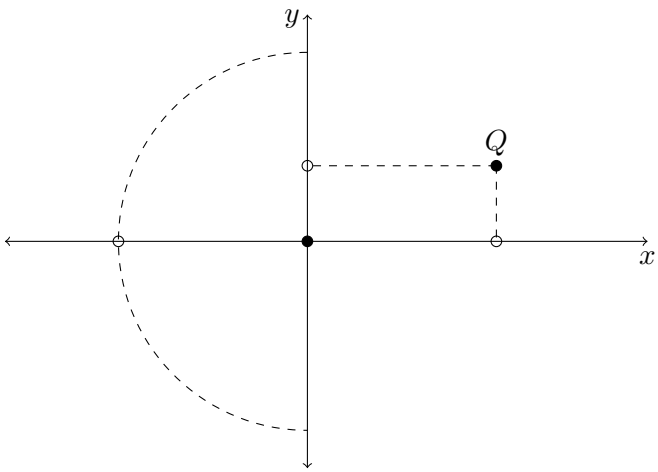


Figura 7.12: Simétrico y proyecciones sobre los ejes.

7.3.4 Lema. Sea $\{(0,0),(1,0)\} \subseteq M \subseteq \mathbb{R}^2$. Entonces,

(1) Si $P = (x_1, y_1)$, $Q = (x_2, y_2) \in C(M)$, entonces $P + Q := (x_1 + x_2, y_1 + y_2) \in C(M)$.

(2) Si $(x, y) \in C(M)$, entonces $(-x, -y) \in C(M)$.

(3) Si $(x, y) \in C(M)$, entonces $(x, -y) \in C(M)$.

Demostración.

(1) Dados dos puntos construibles $P = (x_1, y_1)$ y $Q = (x_2, y_2)$, se trazan la recta que pasa por el origen y por P y la recta paralela a esta que pase por el punto Q. Seguidamente se trazan la recta que pasa el origen y por Q y la recta paralela a este segmento que pase por P. Esas dos rectas se cortan en un punto $P + Q$ cuyas coordenadas son $(x_1 + x_2, y_1 + y_2)$.

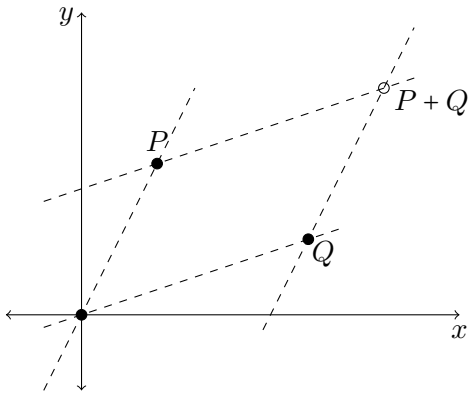


Figura 7.13: Suma de puntos.

(2) Sea $P = (x, y) \in C(M)$. Se traza inicialmente la recta que pasa por el origen y por P. Luego se traza la circunferencia con centro en el origen y radio la distancia entre el origen y P. El segundo punto de corte de esta con la recta es el punto $-P := (-x, -y)$.

(3) Para construir $\overline{P} = (x, -y)$, se traza la recta paralela al eje y que pasa por P y se tiene la proyección $Q = (x, 0)$. Haciendo centro en Q se traza la circunferencia con radio la distancia entre P y Q. Esta corta a la recta anterior en el punto $\overline{P} = (x, -y)$.

Los puntos construibles a partir de un conjunto $M \subseteq \mathbb{R}^2$ y el cuerpo de los números complejos están relacionados de manera sorprendente. Sabemos que cada punto del plano

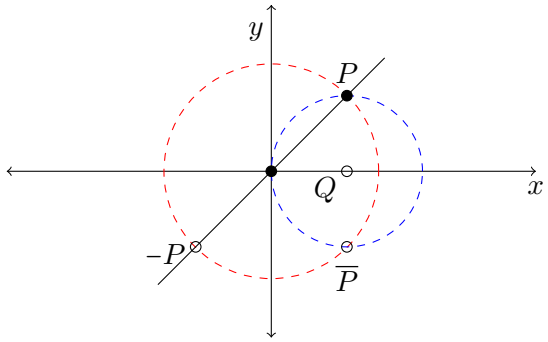


Figura 7.14: Inverso aditivo y conjugado.

euclidiano puede representarse como un número complejo y recíprocamente. En efecto, es suficiente considerar la función

$$\phi : \mathbb{R}^2 \longrightarrow \mathbb{C}$$

definida por

$$\phi(x, y) = x + y\mathrm{i}.$$

Entonces para simplificar consideraremos a $C(M)$ como un subconjunto de $\mathbb{C}$.

7.3.5 Lema. Sea $\{0, 1\} \subseteq M \subseteq \mathbb{C}$. Entonces, $C(M)$ es un subcuerpo de $\mathbb{C}$ que satisface las siguientes condiciones:

(1) $M \subseteq C(M)$.

(2) Si $z \in C(M)$, entonces $\sqrt{z} \in C(M)$.

(3) Si $z \in C(M)$, entonces $\overline{z} \in C(M)$.

Demostración. Sean $z_1, z_2 \in C(M)$ y supongamos que sus representaciones polares están dadas por $z_1 = re^{\mathrm{i}\varphi}$ y $z_2 = se^{\mathrm{i}\psi}$. Entonces,

$$z_1 z_2 = rse^{\mathrm{i}(\varphi+\psi)}$$
$$z_1^{-1} = \frac{1}{r}e^{-\mathrm{i}\varphi}$$
$$\sqrt{z_1} = \sqrt{r}e^{\mathrm{i}\frac{\varphi}{2}}$$

Del lema 7.3.4 se sigue que $-z_1$, $\overline{z}_1$, $z_1 + z_2 \in C(M)$. Resta demostrar que $z_1 z_2$, y z_1^{-1} son elementos construibles y que $C(M)$ satisface (1) y (2).

(1) Para construir $z_1 z_2$ procedemos de la siguiente manera:

- Se traza la circunferencia con centro en el origen y radio 1 y obtenemos el punto D.
- Se construye la recta L_1 que pasa por D y z_2.
- Se traza la circunferencia con centro en el origen y radio r. El punto de corte de esta con el eje y lo notamos con E.
- Se construye la recta L_2 que es paralela a L_1 y que pasa por E. La recta L_3 que pasa por el origen y que contiene a z_2 se intersecta con L_2 en un punto, digamos H. Sea a la distancia del origen al punto H. Aplicando el teorema de Thales se tiene que $\frac{1}{r} = \frac{s}{a}$. Por lo tanto, $a = rs$.
- Se traza la circunferencia con centro en el origen y radio a. De esta manera, tenemos construida la norma del vector buscado.

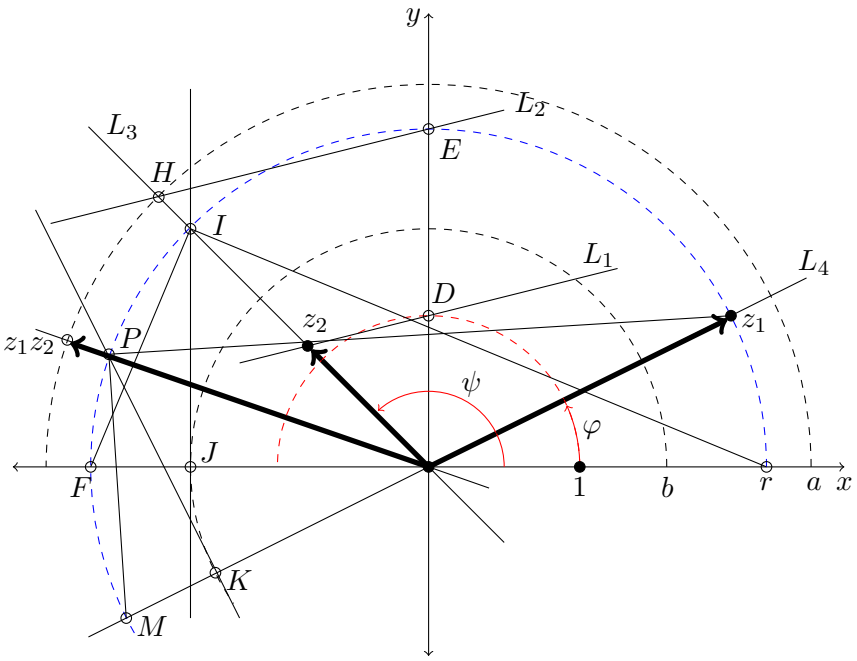


Figura 7.15: Construcción de $z_1 z_2$.

Para construir el ángulo $\varphi + \psi$ procedemos de la siguiente manera:

- La recta L_3 intersecta a la circunferencia con centro en el origen y radio r en un punto I. Se construye la recta perpendicular al eje x que pasa por I. Esta recta corta al eje x en un punto J. Notemos con b la distancia del origen a J.

- Se trazan la circunferencia con centro en el origen y radio b y la recta L_4 que pasa por el origen y que contiene a z_1. Estas se intersectan en un punto K.
- Se traza la recta perpendicular a L_4 que pasa por K. Esta recta intersecta a la circunferencia con centro en el origen y radio r en un punto P.
- Se traza la recta que pasa por el origen y por P. La intersección de esta recta y la circunferencia con radio a es el punto buscado.

(2) Para construir z_1^{-1} procedemos de la siguiente manera:

- Se traza la circunferencia C_1 con centro en $(0,0)$ y radio r y obtenemos el punto ir.
- Se traza la circunferencia con centro en $(0,0)$ y radio 1 y construimos así el punto i.
- Se traza la recta que pasa por $(0,r)$ y $(1,0)$.
- Se traza la recta paralela a la anterior, que pasa por $(0,1)$. Esta recta corta al eje x en $(a,0)$. Aplicando nuevamente el teorema de Thales se tiene que $\frac{r}{1} = \frac{1}{a}$. Por lo tanto, $a = r^{-1}$.
- Se traza la circunferencia C_2 con centro en el origen y radio a. De esta manera, tenemos construida la norma del vector buscado.

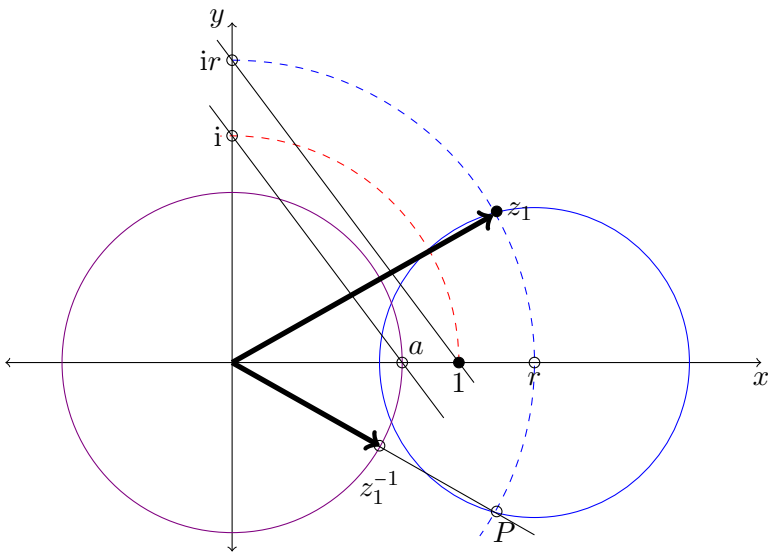


Figura 7.16: Construcción de z_1^{-1}.

Para construir el ángulo $-\varphi$ procedemos de la siguiente manera:

- Sea b la distancia de z_1 al punto $(r,0)$. Se traza ahora la circunferencia C_3 con centro en $(r,0)$ y radio b.
- Sea P el segundo punto de corte de las circunferencias C_1 y C_3. Seguidamente se traza la recta que pasa por el origen y por P.
- La intersección de esta recta y la circunferencia C_2 es el punto buscado.

(3) Para construir $\sqrt{z_1}$ procedemos de la siguiente manera:

- Sea traza la circunferencia C_1 con centro en el origen y radio r.
- Sea traza la circunferencia unitaria, para construir el punto $(-1,0)$.
- Se construye el punto medio M entre $(-1,0)$ y $(r,0)$ y luego se traza la circunferencia C_2 con centro en M y radio la distancia entre M y $(r,0)$. Esta circunferencia corta al eje y en un punto H, digamos $(0,a)$. Se verifica sin dificultades que $a = \sqrt{r}$.
- Se traza la circunferencia C_3 con centro en el origen y radio a. De esta manera tenemos construida la norma del vector buscado.
- El ángulo $\frac{\varphi}{2}$ se obtiene mediante una biseccion del ángulo φ.

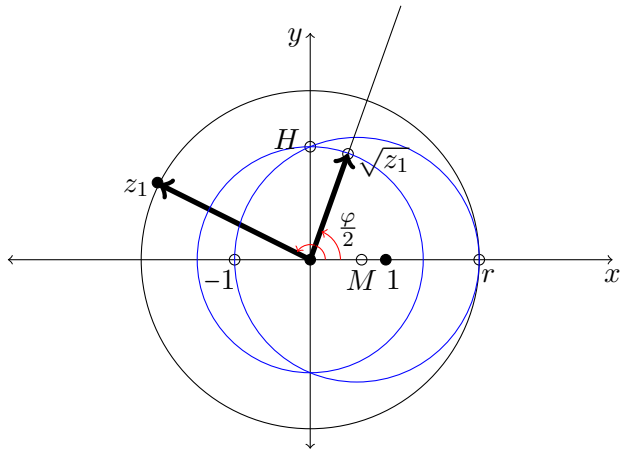


Figura 7.17: Construcción de $\sqrt{z_1}$.

El resto de la demostración es claro. □

7.3.6 Lema. Sea $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Entonces, $C(M)$ es la intersección de todos los subcuerpos K de $\mathbb{C}$ que satisfacen las siguientes condiciones:

(1) $M \subseteq K$.

(2) Si $z \in K$, entonces $\sqrt{z} \in K$.

(3) Si $z \in K$, entonces $\overline{z} \in K$.

DEMOSTRACIÓN. En el lema anterior se demostró que $C(M)$ es un subcuerpo de $\mathbb{C}$ que satisface (1), (2) y (3).

Sea ahora K un subcuerpo cualquiera de $\mathbb{C}$ que satisface (1), (2) y (3). Demostramos que $C(M) \subseteq K$. Para ello consideramos dos afirmaciones intermedias:

1. $x + y\mathrm{i} \in K$ si y solo si $x, y \in K$.

   Supongamos que $x, y \in K$. De (2) se sigue que $\sqrt{-1} = \mathrm{i} \in K$. Por lo tanto, dado que K es un cuerpo se sigue que $x + y\mathrm{i} \in K$.

   Recíprocamente, supongamos que $z = x + y\mathrm{i} \in K$. De (3) se sigue que $\overline{z} = x - y\mathrm{i} \in K$. Por lo tanto, $z + \overline{z} = 2x \in K$. En consecuencia, $x \in K$. Similar se demuestra que $y \in K$.

2. Los otros pasos hacen referencia a las ecuaciones de rectas y circunferencias determinadas por puntos de K. Sean $z_1, z_2 \in K$, digamos $z_1 = x_1 + y_1\mathrm{i}$ y $z_2 = x_2 + y_2\mathrm{i}$.

   La recta que pasa por z_1 y z_2 tiene la ecuación

   $$(y - y_2) = \frac{y_2 - y_1}{x_2 - x_1}(x - x_2).$$

   O equivalentemente

   $$ax + by + c = 0 \tag{7.2}$$

   con $a, b, c \in \mathbb{R} \cap K$ adecuados.

   La circunferencia con centro en $z = a + b\mathrm{i} \in K$ y radio $r \in K$ tiene ecuación

   $$(x - a)^2 + (y - b)^2 = r^2.$$

   O equivalentemente

   $$x^2 + y^2 + dx + ey + f = 0 \tag{7.3}$$

   con $d, e, f \in \mathbb{R} \cap K$ adecuados.

3. Demostramos por inducción matemática sobre n que $M_n \subseteq K$ para todo $n \in \mathbb{N}_0$.

   `Paso 1.` Si $n = 0$, entonces de (1) se sigue que $M_0 = M \subseteq K$.

   `Hipótesis inductiva.` Supongamos que $M_n \subseteq K$.

   Demostramos que $M_{n+1} = M_n^+ \subseteq K$. Para ello consideramos los tres casos posibles:

`Caso 1.` Sea $z \in M_{n+1}$ el punto de intersección de dos rectas no paralelas que se construyen a partir de puntos de M_n. Entonces, z está dado por la solución de un sistema de dos ecuaciones lineales de la forma (7.2) con coeficientes en $\mathbb{R} \cap K$. Utilizando, por ejemplo, la regla de Cramer se tiene que la parte real y la parte imaginaria de z pertenecen a K. Por lo tanto, de (2) se sigue que $z \in K$.

`Caso 2.` Sea $z = u + v\mathrm{i} \in M_{n+1}$ un punto de intersección de una recta de la forma

$$ax + by + c = 0, \quad a, b, c \in \mathbb{R} \cap K, \ b \neq 0$$

con una circunferencia de la forma (7.3). Entonces, $u = \mathrm{Re}(z)$ es solución de una ecuación cuadrática con coeficientes en K. De (2) se sigue que $u \in K$. Dado que $u \in K$ y $au + bv + c = 0$, se tiene que $v \in K$. Usando nuevamente (2) se sigue que $z \in K$.

En el caso $b = 0$ y $a \neq 0$ se sigue análogamente que $z \in K$.

`Caso 3.` Sea $z \in M_{n+1}$ un punto de intersección de dos circunferencias de la forma

$$x^2 + y^2 + dx + ey + f = 0$$

y

$$x^2 + y^2 + d'x + e'y + f' = 0.$$

Entonces, z está sobre la recta

$$(d - d')x + (e - e')y + (f - f') = 0.$$

Note que los coeficientes de esta recta pertenecen a K. Entonces el punto de intersección de esta recta con las circunferencias dadas pertenecen a K como se demostró en el caso anterior.

En resumen tenemos que $M_{n+1} = M_n^+ \subseteq K$. Es decir $C(M) \subseteq K$. □

El anterior lema demuestra que $C(M)$ es el subcuerpo más pequeño de $\mathbb{C}$ que tiene las propiedades (1), (2) y (3).

7.3.7 Lema. Sea K un cuerpo con $\mathrm{char}(K) \neq 2$ y sea L una extensión cuadrática de K. Entonces existe $c \in L$ tal que $L = K(c)$ y $c^2 \in K$.

Demostración. Sea $v \in L \setminus K$. Dado que $\dim_K L = 2$, se verifica que el sistema $B = (1, v, v^2)$ es linealmente dependiente. Por lo tanto, existen $a, b \in K$ tales que

$$v^2 + av + b = 0.$$

Si definimos $c := v + \frac{a}{2}$, entonces se tiene que

$$c^2 = \underbrace{v^2 + av}_{=-b \in K} + \frac{a^2}{4} \in K.$$

Si $c \in K$, entonces $v = c - \frac{a}{2} \in K$, una contradicción. Por lo tanto, $c \notin K$ y se tiene usando la fórmula del grado que $K(c) = L$. $\square$

7.3.8 Definición. Sea $M \subseteq \mathbb{C}$. Definimos $\overline{M} \subseteq \mathbb{C}$ de la siguiente manera:

$$\overline{M} = \{\overline{z} \mid z \in M\}.$$

7.3.9 Lema. Sea $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Entonces, $a \in C(M)$ si y solo si existen subcuerpos $K_1, \ldots, K_n$ de $\mathbb{C}$ con las siguientes propiedades:

(a') $\mathbb{Q}(M \cup \overline{M}) =: K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$.

(b') $|K_j : K_{j-1}| = 2$ para todo $j = 1, \ldots n$.

(c') $a \in K_n$.

Demostración. Supongamos que están dados subcuerpos $K_1, \ldots, K_n$ de $\mathbb{C}$ con las propiedades (a'), (b') y (c'). Usando inducción matemática demostramos a continuación que $K_j \subseteq C(M)$ para todo $j = 0, 1, \ldots, n$.

Del lema 7.3.6 se sigue que $K_0 \subseteq C(M)$.

Como hipótesis inductiva, supongamos que está demostrado que

$$K_j \subseteq C(M).$$

Del lema 7.3.7 se sigue que existe $c \in K_{j+1}$ tal que $c^2 \in K_j$ y $K_{j+1} = K_j(c)$. Usando nuevamente el lema 7.3.6 se tiene que $c \in C(M)$ con lo cual podemos afirmar que

$$K_{j+1} = K_j(c) \subseteq C(M).$$

En consecuencia, $a \in K_n$ y, por lo tanto, $a \in C(M)$.

Recíprocamente, sea Ω el conjunto de todos los $a \in \mathbb{C}$ para los cuales existen subcuerpos $K_1, \ldots, K_n$ de $\mathbb{C}$ con las propiedades (a'), (b') y (c').

`Afirmación:` Ω es un subcuerpo de $\mathbb{C}$ con las propiedades (1), (2) y (3) del lema 7.3.6.

En efecto, sean $a, b \in \Omega$ con $a \neq 0$ y digamos que

$$K_0 \subseteq K_0(a_1) \subseteq K_0(a_1, a_2) \subseteq \cdots \subseteq K_0(a_1, \ldots, a_r) \ni a$$

$$K_0 \subseteq K_0(b_1) \subseteq K_0(b_1, b_2) \subseteq \cdots \subseteq K_0(b_1, \ldots, b_s) \ni b,$$

donde $a_{j+1}^2 \in K_0(a_1, \ldots, a_j)$ y $b_{j+1}^2 \in K_0(b_1, \ldots, b_j)$.

Se verifica que

$$K_0 \subseteq K_0(a_1) \subseteq \cdots \subseteq K_0(a_1, \ldots, a_r) \subseteq \cdots \subseteq K_0(a_1, \ldots, a_r, b_1, \ldots, b_s).$$

Si definimos $F := K_0(a_1, \ldots, a_r, b_1, \ldots, b_s)$, entonces tenemos que $a, b \in F$. Además para cada subcuerpo E de F en la cadena anterior se verifica que $|F : E| \leq 2$. Es decir, $E = F$ o $|F : E| = 2$, con lo cual concluimos que $a \pm b$, ab, $a^{-1} \in F \subseteq \Omega$, así se tiene que Ω es un subcuerpo de $\mathbb{C}$.

Dado que $M \subseteq \Omega$, de (a') se sigue (1).

Si $z \in K_n$, siendo K_n como en la hipótesis, entonces se sigue que

$$|K_n(\sqrt{z}) : K_n| \leq 2,$$

con lo cual afirmamos que $\sqrt{z} \in \Omega$. Esto demuestra que Ω satisface (2).

Para demostrar (3), sean $a \in \Omega$ y $K_1, \ldots, K_n$ como en la hipótesis del teorema. Sea τ la función conjugación. Dado que τ es un automorfismo de $\mathbb{C}$, se sigue que $\overline{K_j} = \tau(K_j)$ es un subcuerpo de $\mathbb{C}$ para todo $j = 1, \ldots, n$. Dado además que $\tau(\mathbb{Q}) = \mathbb{Q}$ y $\tau(M \cup \overline{M}) = M \cup \overline{M}$, se sigue que $K_0 \subseteq \tau(K_0)$. También se verifica que

$$\tau(K_0) \subseteq \tau^2(K_0) = K_0.$$

Es decir, $\tau(K_0) = K_0$.

De $K_{j+1} = K_j + a_j K_j$ y $a_j^2 \in K_j$ (ver lema anterior) se sigue que

$$\overline{K}_{j+1} = \overline{K}_j + \overline{a}_j \overline{K}_j \text{ con } \overline{a}_j^2 \in \overline{K}_j,$$

con lo cual, usando el lema 7.3.6 se tiene que $|\overline{K}_{j+1} : \overline{K}_j| \leq 2$. Esto trae como consecuencia que $\bar{a} \in \overline{K}_n \subseteq \Omega$ demostrando la afirmación.

Usando nuevamente el lema 7.3.6 se sigue que $C(M) \subseteq \Omega$, concluyendo así la demostración del teorema. □

El siguiente resultado establece el grado de los elementos construibles, el cual es de gran ayuda para la insolubilidad de los tres problemas clásicos.

7.3.10 Corolario. Sean $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ y $K_0 := \mathbb{Q}(M \cup \overline{M})$ dados. Si $a \in \mathbb{C}$ es construible con regla y compás a partir de M, entonces $|K_0(a) : K_0| = 2^m$ para algún $m \in \mathbb{N}_0$.

Demostración. Si $a \in L$ para algún subcuerpo L de $\mathbb{C}$ que sea extensión de K_0, entonces del lema anterior y de la fórmula del grado se sigue que

$$|L : K_0| = 2^n$$

para algún $n \in \mathbb{N}_0$. Entonces el grado del cuerpo intermedio $K_0(a)$ de la extensión L/K_0 sobre K_0 es una potencia de 2. □

7.4 Los tres problemas clásicos

Duplicación del cubo

Sean $M = \{0, 1\}$ y $K_0 = \mathbb{Q}$. Sin perder generalidad, supongamos que el cubo tiene volumen 1. Para duplicar el volumen del cubo se hace necesario construir un segmento con longitud $a = \sqrt[3]{2}$. Es decir, es necesario construir con regla y compás el número $\sqrt[3]{2}$. Pero, el polinomio minimal $m_{a,\mathbb{Q}} = x^3 - 2$ y, por lo tanto, $|\mathbb{Q}(a) : \mathbb{Q}| = 3$, lo cual por el corolario anterior no es posible, ya que 3 no es una potencia de 2.

Cuadratura del círculo

Sean $M = \{0, 1\}$ y $K_0 = \mathbb{Q}$. Sin perder generalidad, supongamos que el círculo tiene radio 1. En este caso se tiene que el área del círculo es π. Es decir, buscamos un cuadrado con lado $\sqrt{\pi}$.

Si $\sqrt{\pi} \in C(M)$, entonces $\pi \in C(M)$, por lo tanto $|\mathbb{Q}(\pi) : \mathbb{Q}|$ sería finito, lo cual es imposible por la trascendencia de π sobre $\mathbb{Q}$.

La trisección de un ángulo

En general no todo ángulo puede trisecarse con regla y compás. En efecto, demostramos a continuación que esto no es posible para un ángulo de 60°. Para ello, sean $M = \{0, 1\}$ y $K_0 = \mathbb{Q}$.

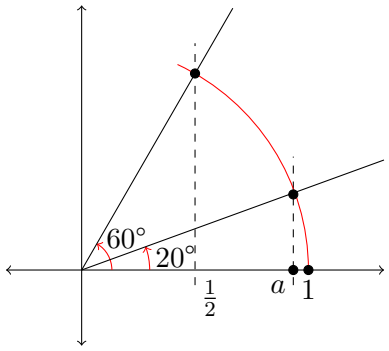


Figura 7.18: Trisección de un ángulo.

Un ángulo de 60° puede trisecarse si $a := \cos 20°$ es construible con regla y compás.

Comparando las partes reales e imaginarias de

$$\cos 3\alpha + i \sin 3\alpha = e^{i3\alpha} = (e^{i\alpha})^3 = (\cos\alpha + i \sin\alpha)^3$$

se tiene la identidad trigonométrica

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha,$$

la cual para $\alpha = 30°$ y $a := \cos 20°$ suministra la igualdad

$$\frac{1}{2} = 4a^3 - 3a.$$

Por lo tanto, a es una raíz del polinomio $f = 8x^3 - 6x - 1$. Se verifica que f es irreducible sobre $\mathbb{Q}$. En consecuencia, $|\mathbb{Q}(a) : \mathbb{Q}| = 3$ y se tiene que a no es construible con regla y compás.

7.5 Ejercicios

(1) Sea $\{0, 1\} \subseteq M \subseteq \mathbb{C}$.

   (a) ¿Es la extensión $Cons(M)/\mathbb{Q}(M \cup M\overline{M})$ algebraica?

   (b) Demuestre que $|Cons(M) : \mathbb{Q}| = \infty$.

(2) Considere dada la ecuación

$$x^2 + px + q = 0, \quad \text{con} \quad p, q \in \mathbb{R}.$$

   Usando regla y compás construya a partir del conjunto $\{0, 1, p, q\}$ las soluciones complejas x_1, x_2 de dicha ecuación.

APÉNDICE A

EL ANILLO DE POLINOMIOS

A lo largo de este capítulo R denota siempre un anillo conmutativo.

A.1 Polinomios en una indeterminada

A.1.1 Definición. Sea $f : \mathbb{N}_0 \longrightarrow R$. Definimos `el soporte` de f, notado con $\text{sop}(f)$, de la siguiente manera:

$$\text{sop}(f) := \{n \in \mathbb{N}_0 \mid f(n) \neq 0\}.$$

Si $\text{sop}(f)$ es un conjunto finito, entonces decimos que f tiene `soporte finito`. Notaremos con $P(R)$ al conjunto de todas las sucesiones sobre R que tienen soporte finito. Esto es:

$$P(R) = \{(a_j)_{j\in\mathbb{N}_0} \mid a_j \in R,\ a_j = 0,\ \text{para casi todo } j\}.$$

Todo elemento de $P(R)$ de la forma $(a, 0, 0, \ldots)$ se denomina una `constante` de $P(R)$.

A.1.2 Observación. Sobre el conjunto $P(R)$ definamos las siguientes operaciones:

Sean $a = (a_j)_{j\in\mathbb{N}_0}$ y $b = (b_j)_{j\in\mathbb{N}_0}$ elementos de $P(R)$. Entonces,

$$a + b := (s_j)_{j\in\mathbb{N}_0},\ \text{donde } s_j = a_j + b_j \text{ para todo } j \in \mathbb{N}_0$$

$$a \cdot b := (c_k)_{k\in\mathbb{N}_0},\ \text{donde } c_k = \sum_{i=0}^{k} a_i b_{k-i} \text{ para todo } k \in \mathbb{N}_0.$$

Se verifica sin dificultades que $a+b$ y $a\cdot b \in P(R)$. Sean $a = (a_j)_{j\in\mathbb{N}_0}$ y $b = (b_j)_{j\in\mathbb{N}_0} \in P(R)$, $a + b = (s_j)_{j\in\mathbb{N}_0}$ y $a \cdot b = (c_k)_{k\in\mathbb{N}_0}$. Entonces,

(1) Si $a_j = 0$ para todo $j > m$ y $b_j = 0$ para todo $j > n$, entonces $s_j = 0$ para todo $j > \max\{m, n\}$.

(2) Si $a_i = 0$ para todo $i > m$ y $b_j = 0$ para todo $j > n$, entonces $c_k = 0$ para todo $k > m + n$. En efecto, si $k > m + n$, entonces se tiene que

$$c_k = \sum_{i=0}^{m} a_i \underbrace{b_{k-i}}_{=0} + \sum_{i=m+1}^{k} \underbrace{a_i}_{=0} b_{k-i} = 0.$$

Observe que la definición de la multiplicación también puede expresarse de la siguiente manera:

$$a \cdot b = (c_k)_{k\in\mathbb{N}_0}, \text{ donde } c_k = \sum_{i+j=k} a_i b_j \text{ para todo } k \in \mathbb{N}_0.$$

A.1.3 Lema. Con las operaciones descritas anteriormente se verifica que $P(R)$ es un anillo conmutativo con elemento identidad.

Demostración. La verificación de los axiomas de anillo no es difícil, simplemente es tediosa. Es claro que el cero está dado por la sucesión nula. Es decir, $0 = (0, 0, \ldots)$. El elemento identidad está dado por $1 = (1, 0, 0, \ldots)$.

Verificamos la asociatividad del producto: sean $a = (a_i)_{i\in\mathbb{N}_0}$, $b = (b_j)_{j\in\mathbb{N}_0}$ y $c = (c_k)_{k\in\mathbb{N}_0}$ elementos de $P(R)$. Entonces, $(ab)c = (d_l)_{l\in\mathbb{N}_0}$, donde

$$d_l = \sum_{r+k=l} \Big(\sum_{i+j=r} a_i b_j \Big) c_k = \sum_{i+j+k=l} (a_i b_j) c_k$$

y $a(bc) = (f_l)_{l\in\mathbb{N}_0}$, donde

$$f_l = \sum_{i+s=l} a_i \Big(\sum_{j+k=s} b_j c_k \Big) = \sum_{i+j+k=l} (a_i b_j) c_k,$$

con lo cual se tiene la afirmación. □

Demostramos a continuación que el anillo R puede considerarse un subanillo de $P(R)$. Es decir, podemos sumergir a R en el anillo $P(R)$.

A.1.4 Lema. La función $\varphi : R \longrightarrow P(R)$ definida por

$$\varphi(r) = (r, 0, 0, \ldots)$$

es un monomorfismo de anillos.

DEMOSTRACIÓN. Es claro que $\operatorname{sop}(\varphi(r))$ es un conjunto finito. Sean además $a, b \in R$. Se verifica sin dificultades que $\varphi(a+b) = \varphi(a) + \varphi(b)$ y $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Por otro lado,

$$\begin{aligned} r \in \ker(\varphi) &\Leftrightarrow (r, 0, 0, \ldots) = (0, 0, 0, \ldots) \\ &\Leftrightarrow r = 0, \end{aligned}$$

lo cual demuestra la inyectividad de φ. □

Otra forma alternativa para representar los elementos de $P(R)$ es la muy conocida `notación de polinomios`

$$\sum_{j=0}^{n} a_j x^j$$

en la `indeterminada` x, donde x es un elemento de $P(R)$.

A.1.5 Definición. Sea $x : \mathbb{N}_0 \longrightarrow R$ definida de la siguiente manera:

$$x = (a_j)_{j \in \mathbb{N}_0},$$

donde $a_j = 0$ para todo $j \neq 1$ y $a_1 = 1$. Es decir,

$$x = (0, 1, 0, \ldots).$$

Note que $\operatorname{sop}(x)$ es un conjunto finito, por lo tanto $x \in P(R)$.

A.1.6 Lema. Si las potencias naturales de la indeterminda x se definen de manera recursiva como sigue:

$$x^n := \begin{cases} (1, 0, 0 \ldots) & \text{si} \quad n = 0 \\ x x^{n-1} & \text{si} \quad n \geq 1, \end{cases} \tag{A.1}$$

entonces,

$$x^n = (0, 0, \ldots, 0, 1, 0, \ldots),$$

donde el 1 se encuentra en la n-ésima posición.

DEMOSTRACIÓN. Se demuestra la afirmación por inducción matemática sobre n. Si $n = 0$, entonces se tiene la afirmación inmediatamente.

`Hipótesis inductiva.` Supongamos que se ha demostrado que

$$x^{n-1} = (\delta_{0,n-1}, \delta_{1,n-1}, \ldots).$$

Entonces, $x^n = x x^{n-1} = (a_0, a_1, \ldots)$, donde

$$a_k = \sum_{j=0}^{k} \delta_{j1} \delta_{k-j,n-1} = \delta_{11} \delta_{k-1,n-1} = \begin{cases} 1, & \text{si} \quad k = n \\ 0, & \text{en otro caso,} \end{cases}$$

con lo cual se tiene la afirmación. □

Dado que R puede verse como un subanillo de $P(R)$, para $a \in R$ se verifica que

$$a = (a, 0, 0, \ldots) = a(1, 0, 0 \ldots) = ax^0.$$

Además,

$$ax^n = (0, \ldots, 0, a, 0 \ldots),$$

donde a se encuentra en la n-ésima posición. En consecuencia, para cualquier $f \in P(R)$, digamos $f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ se verifica que

$$f = \sum_{j=0}^{n} a_j x^j. \tag{A.2}$$

Observe que la notación (A.2) no es más que la función $f : \mathbb{N}_0 \longrightarrow R$ definida por $f(j) = a_j$. Por consiguiente, se tiene la posibilidad de comparar coeficientes. Esto es:

$$\sum_{j \in \mathbb{N}_0} a_j x^j = \sum_{j \in \mathbb{N}_0} b_j x^j \Leftrightarrow a_j = b_j, \text{ para todo } j \in \mathbb{N}_0.$$

Con esta notación las operaciones definidas sobre $P(R)$ pueden escribirse de la siguiente manera:

$$\sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{m} b_j x^j = \sum_{j=0}^{\max\{m,n\}} (a_j + b_j) x^j$$

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{m+n} \Big(\sum_{i=0}^{k} a_i b_{k-i} \Big) x^k$$

`Notación.` En adelante con relación al anillo, en lugar de $P(R)$ escribiremos $R[x]$ y lo llamaremos el anillo de `los polinomios` sobre R en la `indeterminada` x. Los elementos de $R[x]$ se denominan `polinomios` sobre R en x.

A.1.7 Observación. (Diferencia entre polinomios y funciones polinómicas)

1. Una función $f : R \longrightarrow R$ se denomina `polinómica` si existen $m \in \mathbb{N}_0$ y $a_0, \ldots, a_m \in R$ tales que para todo $t \in R$
$$f(t) = \sum_{j=0}^{m} a_j t^j.$$

2. Los polinomios no son funciones de R en R.

Note que a cada polinomio puede asociarse una función polinómica y es posible que polinomios distintos definan la misma función. Por ejemplo, si R es el cuerpo binario $\mathbb{F}_2$, entonces las funciones polinómica $f_1(t) = t^2 + t$ y $f_2(t) = t^2 - t$ tienen asociado el mismo polinomio $f = (0, 1, 1, 0 \ldots)$.

A.1.8 Definición. Sean R un anillo conmutativo y $f \in R[x]$, digamos $f = \sum_{j\in\mathbb{N}_0} a_j x^j$. Definimos `el grado` de f, notado con $\operatorname{grad}(f)$, de la siguiente manera:

$$\operatorname{grad}(f) := \begin{cases} \max\{j \in \mathbb{N}_0 \mid a_j \neq 0\}, & \text{si } f \neq 0 \\ -\infty, & \text{si } f = 0. \end{cases}$$

Si $f = \sum_{j=0}^{n} a_j x^j$ y $\operatorname{grad}(f) = n$, entonces $a_n \neq 0$ y se denomina el `coeficiente principal` de f y si $a_n = 1$, entonces decimos que f es un polinomio `mónico`.

Como es usual en el análisis, acordaremos que para todo $n \in \mathbb{N}$

$$-\infty < n, -\infty + n = -\infty + (-\infty) = n + (-\infty) = -\infty.$$

A.1.9 Teorema. Sean R un dominio entero y $f, g \in R[x]$. Entonces

(1) $\operatorname{grad}(f + g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$.

(2) $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$.

(3) $R[x]$ es un domino entero.

(4) $U(R[x]) = U(R)$.

Demostración. Supongamos que $f = \sum_{j=0}^{n} a_j x^j$ y $g = \sum_{j=0}^{m} b_j x^j$. Es decir, $\operatorname{grad}(f) = n$ y $\operatorname{grad}(g) = m$. Entonces:

(1) Si f o g o ambos son el polinomio nulo, entonces el resultado es inmediato.

Supongamos entonces que $f \neq 0 \neq g$. Entonces,

$$f + g = \sum_{j=0}^{r} (a_j + b_j) x^j,$$

con $r = \max\{m, n\}$. Por lo tanto, $\operatorname{grad}(f + g) \leq r$.

(2) Si f o g o ambos son el polinomio nulo, entonces el resultado es inmediato.

Supongamos entonces que $f \neq 0 \neq g$ y que $m, n \geq 0$. Entonces:

$$fg = \sum_{k=0}^{m+n} c_k x^k,$$

donde

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Demostramos que $c_{m+n} = a_n b_m$. En efecto,

$$c_{m+n} = \sum_{i=0}^{n-1} a_i \underbrace{b_{m+n-i}}_{=0} + a_n b_m + \sum_{i=n+1}^{m+n} \underbrace{a_i}_{=0} b_{k-i} = 0.$$

Por lo tanto, $c_{m+n} = a_n b_m$ y se tiene que

$$\text{grad}(fg) = \text{grad}(f) + \text{grad}(g).$$

(3) Se sigue inmediatamente de (2), ya que el producto de dos polinomios no nulos no puede ser el polinomio nulo.

(4) Si $a \in U(R)$, entonces $(a, 0, \ldots) \in U(R[x])$. Por lo tanto, $U(R) \subseteq U(R[x])$. Sea $f \in U(R[x])$. Entonces, existe $g \in K[x]$ tal que $fg = 1$. Entonces:

$$0 = \text{grad}(1) = \text{grad}(fg) = \text{grad}(f) + \text{grad}(g).$$

Se sigue entonces que $\text{grad}(f) = \text{grad}(g) = 0$. Es decir, $f, g \in R$ y finalmente $f \in U(R)$. Con lo cual se tiene la igualdad. □

A.1.10 Observación. La hipótesis que R sea un dominio entero es central ya que en general (2) y (4) son falsas. Por ejemplo, si $R = \mathbb{Z}_4$, $f = 2x^2 + 3x + 1$ y $g = 2x^3 + x + 2$, entonces $fg = 2x^4 + x^2 + 3x + 2$. Observe que

$$\text{grad}(fg) = 4 < 5 = \text{grad}(f) + \text{grad}(g).$$

Por otro lado, $(2x + 1)^2 = 1$. Es decir, $2x + 1 \in U(\mathbb{Z}_4[x])$, no obstante $2x + 1 \notin R$.

Similar como en el anillo de los enteros, siempre que R sea un dominio entero se verifica en $R[x]$ el algoritmo de la división con resto. En términos de lenguaje futuro, esto significa que $R[x]$ tiene la propiedad de ser euclidiano.

A.1.11 Teorema. (División con resto) Sean R un dominio entero, $f, g \in R[x]$ con $0 \neq g = \sum_{j=0}^{m} b_j x^j$. Si $b_m \in U(R)$, entonces existen únicos $q, r \in R[x]$ tales que

$$f = gq + r \quad \text{y} \quad \text{grad}(r) < \text{grad}(g).$$

DEMOSTRACIÓN. Sean $f = \sum_{j=0}^{n} a_j x^j$ y $g = \sum_{j=0}^{m} b_j x^j$,

`Existencia.` Si $\text{grad}(f) < \text{grad}(g)$, entonces tómese $q = 0$ y $r = f$ y se tiene el resultado.

Supongamos que $n := \text{grad}(f) \geq \text{grad}(g) =: m$ y que los coeficientes principales de f y g son respectivamente a_n y b_m. Procedemos por inducción sobre n.

`Paso 1.` Si $n = 0$, entonces $f = a_0$ y $g = b_0$ con $b_0 \in U(R)$ y así

$$a_0 = (a_0 b_0^{-1})b_0 + 0.$$

Definiendo $q := a_0 b_0^{-1}$ y $r := 0$ se tiene la afirmación.

`Hipótesis inductiva.` Supongamos que la afirmación es válida para todo $h \in R[x]$ con $\text{grad}(h) < n$. Definamos

$$h := f - a_n b_m^{-1} x^{n-m} g.$$

Es claro que $\text{grad}(h) < n$. Entonces por la hipótesis inductiva se tiene que existen $q_1, r \in R[x]$ tales que

$$h = gq_1 + r, \quad \text{y} \quad \text{grad}(r) < \text{grad}(g).$$

Por lo tanto,

$$\begin{aligned} fh + a_n b_m^{-1} x^{n-m} g &= (gq_1 + r) + a_n b_m^{-1} x^{n-m} g \\ &= g(q_1 + a_n b_m^{-1} x^{n-m}) + r. \end{aligned}$$

Defínase entonces $q := q_1 + a_n b_m^{-1} x^{n-m}$ y se tiene el resultado.

`Unicidad.` Supongamos que $f = gq_1 + r_1 = gq_2 + r_2$ con $\text{grad}(r_1) < \text{grad}(g)$ y $\text{grad}(r_2) < \text{grad}(g)$.

Si $q_1 = q_2$, entonces $r_1 = r_2$ y se tiene el resultado. Supongamos entonces que $q_1 \neq q_2$. En consecuencia, $\text{grad}(q_1 - q_2) \geq 0$.

Por otro lado,

$$\begin{aligned} \text{grad}(g) + \text{grad}(q_1 - q_2) &= \text{grad}(g(q_1 - q_2)) \\ &= \text{grad}(r_2 - r_1) \\ &\leq \max\{\text{grad}(r_1), \text{grad}(r_2)\} \\ &< \text{grad}(g). \end{aligned}$$

Entonces, $\text{grad}(q_1 - q_2) < 0$, lo cual es una contradicción. □

A.1.12 Definición. Sean R y S anillos conmutativos, $R \subseteq S$ y $s \in S$ fijo.

(1) La función $\varphi : R[x] \longrightarrow S$, definida por

$$\varphi(f) = \varphi\Big(\sum_{j=0}^{n} a_j x^j\Big) := \sum_{j=0}^{n} a_j s^j =: f(s)$$

es un homomorfismo de anillos, el cual denominaremos homomorfismo de `sustitución`.

(2) Si $f \in R[x]$ y $f(s) = 0$, entonces decimos que s es `una raíz` o `un cero` de f en S.

A.1.13 Ejemplo. Sea $f = x^2 \in \mathbb{R}[x]$. Consideremos sustituciones por elementos del anillo $\mathrm{Mat}(2, \mathbb{R})$. Sea

$$C = \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}.$$

Entonces se verifica que $C^2 = 0$. Por lo tanto, f tiene infinitas raíces en $\mathrm{Mat}(2, \mathbb{R})$.

A.1.14 Lema. Sean R un dominio entero, $f \in R[x]$ y $a \in R$. Entonces existe $q \in R[x]$ tal que

$$f = (x - a)q + f(a).$$

En particular, si a es una raíz de f, entonces $f = (x - a)q$.

DEMOSTRACIÓN. De la división con resto se sigue que existen $q, r \in R[x]$ tales que

$$f = (x - a)q + r \quad \text{y} \quad \mathrm{grad}(r) < \mathrm{grad}(x - a) = 1.$$

Es decir, $r \in R$. Substituyendo tenemos que $f(a) = r$ con lo cual se tiene la afirmación. □

A.1.15 Teorema. Sea R un dominio entero y $f \in R[x]$ con $\mathrm{grad}(f) = m$.

(1) Si $b_1, \ldots, b_n \in R$ son raíces distintas de f, entonces existe $g \in R[x]$ tal que $f = (x - b_1) \cdots (x - b_n)g$.

(2) f tiene a lo más m raíces distintas en R.

(3) Si $g, h \in R[x]$, $\mathrm{grad}(g), \mathrm{grad}(h) \leq n$ y existen $n + 1$ elementos distintos $b_1, \ldots, b_{n+1} \in R$ tales que $g(b_j) = h(b_j)$, para $j = 1, \ldots, n + 1$, entonces $g = h$.

DEMOSTRACIÓN. (1) Procedemos por inducción sobre n.

Sea $n = 1$. Entonces el resultado se sigue inmediatamente.

`Hipótesis inductiva.` Supongamos que para $k < n$ está demostrado que

$$f = (x - b_1) \cdots (x - b_k)g_k, \quad \text{con} \quad g_k \in R[x].$$

Substituyendo x por b_{k+1} tenemos

$$0 = f(b_{k+1}) = \underbrace{(b_{k+1} - b_1)}_{\neq 0} \cdots \underbrace{(b_{k+1} - b_k)}_{\neq 0} g_k(b_{k+1}).$$

Por lo tanto, $g_k(b_{k+1}) = 0$ y se sigue que

$$g_k = (x - b_{k+1})g_{k+1}, \text{ con } g_{k+1} \in R[x].$$

En resumen se tiene que

$$f = (x - b_1)\cdots(x - b_k)(x - b_{k+1})g_{k+1}.$$

(2) Sean $b_1, \ldots, b_n$ raíces distintas de f. De (a) se sigue que

$$f = (x - b_1)\cdots(x - b_n)g,$$

con lo cual podemos afirmar que

$$m = \text{grad}(f) = \underbrace{1 + \cdots + 1}_{n} + \text{grad}(g) \geq n.$$

Dado que $\text{grad}(g - h) \leq n$ y $(g - h)(b_j) = 0$, para $j = 1, \ldots, n + 1$, se sigue que $g - h = 0$. Es decir, $g = h$. $\square$

A.2 La propiedad universal

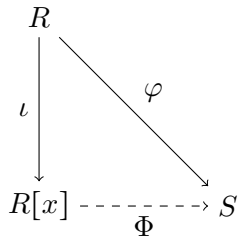
Esta propiedad establece que todo homomorfismo φ de R en otro anillo conmutativo S puede extenderse de una única forma a un homomorfismo de $R[x]$ en S, conociendo únicamente la imagen de x.

A.2.1 Teorema. (La propiedad universal) Sean R y S anillos conmutativos. Si $\varphi : R \longrightarrow S$ es un homomorfismo de anillos con $\varphi(1) = 1$ y $s \in S$ cualquiera, entonces existe un único homomorfismo

$$\Phi : R[x] \longrightarrow S$$

que extiende a φ, es decir, $\Phi\,|_R = \varphi$ y, además, satisface $\Phi(x) = s$.

Ilustración:



DEMOSTRACIÓN. `Existencia.` La función $\Phi : R[x] \longrightarrow S$ definida por

$$\Phi\Big(\sum_{j\in\mathbb{N}_0} a_j x^j\Big) = \sum_{j\in\mathbb{N}_0} \varphi(a_j)s^j \tag{A.3}$$

satisface que $\Phi\,|_R = \varphi$ y $\Phi(x) = s$. Resta demostrar que es un homomorfismo de anillos. Para ello, sean $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j \in R[x]$ y definamos $k := \max\{m, n\}$. Entonces:

$$\begin{aligned}
\Phi(f+g) &= \sum_{j=0}^{k} \varphi(a_j + b_j)s^j \\
&= \sum_{j=0}^{k} (\varphi(a_j) + \varphi(b_j))s^j \\
&= \sum_{j=0}^{n} \varphi(a_j)s^j + \sum_{j=0}^{m} \varphi(b_j)s^j \\
&= \Phi(f) + \Phi(g).
\end{aligned}$$

Supongamos ahora que $f \cdot g = \sum_{k=0}^{m+n} c_k x^k$ con $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Entonces:

$$\begin{aligned}
\Phi(f\cdot g) &= \sum_{k=0}^{m+n} \varphi(c_k)s^k \\
&= \sum_{k=0}^{m+n} \varphi\Big(\sum_{i=0}^{k} a_i b_{k-i}\Big)s^k \\
&= \sum_{k=0}^{m+n} \Big(\sum_{i=0}^{k} \varphi(a_i)\varphi(b_{k-i})\Big)s^k \\
&= \Phi(f)\cdot\Phi(g).
\end{aligned}$$

`Unicidad.` Sea $\hat{\Phi} : R[x] \longrightarrow S$ otro homomorfismo que extiende a φ y que, además, satisface $\hat{\Phi}(x) = s$. Entonces:

$$\hat{\Phi}\Big(\sum_{j=0}^{n} a_j x^j\Big) = \sum_{j=0}^{n} \hat{\Phi}(a_j)\hat{\Phi}(x)^j = \sum_{j=0}^{n} \varphi(a_j)s^j = \Phi\Big(\sum_{j=0}^{n} a_j x^j\Big).$$

En consecuencia, $\hat{\Phi} = \Phi$. □

A.2.2 Ejemplo. Sean $R = \mathbb{R}$, $S = \mathbb{C}$ y $s = \mathrm{i}$. Del teorema anterior se sigue que la función $\Phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ definida por $\Phi(f) = f(\mathrm{i})$ es un homomorfismo de anillos. Además, Φ es sobreyectiva. En efecto, dado $z \in \mathbb{C}$, digamos $z = a + b\mathrm{i}$, entonces $z = \Phi(f)$ con $f = a + bx$.

A.2.3 Definición. Si R es un dominio entero, entonces del teorema anterior se sigue que $R[x]$ también lo es, por lo tanto $R[x]$ admite un cuerpo cociente, el cual notamos con $R(x)$. Esto es,

$$R(x) \coloneqq Q(R[x]) = \left\{ \frac{f}{g} \mid f, g \in R[x],\ g \neq 0 \right\}.$$

Llamaremos a $R(x)$ el cuerpo de las `funciones racionales`.

A.3 Polinomios en varias indeterminadas

Demostramos anteriormente que, si R es un anillo conmutativo, entonces $R[x]$ también lo es. Esto significa que podemos formar el anillo $R[x_1, x_2] \coloneqq R[x_1][x_2]$.

Un elemento de $R[x_1, x_2]$ es una sucesión $(a_j)_{j \in \mathbb{N}_0}$, donde cada $a_j \in R[x_1]$ y solo un número finito de estos son no nulos. Nuevamente, usando el monomorfismo

$$\varphi : R[x_1] \longrightarrow R[x_1, x_2]$$

definido por $\varphi(a) \coloneqq (a, 0, 0 \ldots)$ puede sumergirse el anillo $R[x_1]$ en $R[x_1, x_2]$. Dado que R puede considerarse también subanillo de R se tiene la cadena de anillos:

$$R \subseteq R[x_1] \subseteq R[x_1, x_2].$$

Similar como caracterizamos los elementos del anillo $R[x]$, cada elemento $f \in R[x_1, x_2]$ puede representarse de manera única en la forma

$$f = \sum_{j=0}^{n} g_j x_2^j$$

donde cada $g_j \in R[x_1]$. Si escribimos $g_j = \sum_{i=0}^{m} a_{ij} x_1^i$ con $a_{ij} \in R$, entonces f tiene la representación

$$f = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x_1^i x_2^j, \quad \text{con} \quad a_{ij} \in R.$$

A.3.1 Observación. Es importante tener cuidado en la notación. Por ejemplo, $x_2 = (0, 1, 0, 0, \ldots)$ y $x_1 \in R[x_1, x_2]$ está dado por la sucesión $(x_1, 0, 0, \ldots)$.

Este procedimiento puede extenderse de manera inductiva y obtener el anillo de los polinomios en n indeterminadas $x_1, \ldots, x_n$ de la siguiente manera:

$$R[x_1, \ldots, x_n] \coloneqq R[x_1, \ldots, x_{n-1}][x_n].$$

Como en el caso de dos indeterminadas, identificando $g \in R[x_1, \ldots, x_{n-1}]$ con la sucesión $(g_1, 0, 0, \ldots) \in R[x_1, \ldots, x_n]$, se tiene que todo elemento $f \in R[x_1, \ldots, x_n]$ puede representarse de manera única en la forma

$$f = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n},$$

con $a_{i_1 \ldots i_n} \in R$ y solo un número finito de estos es no nulo.

En resumen, $R[x_1, \ldots, x_n]$ es el conjunto

$$\Big\{ \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \mid a_{i_1 \ldots i_n} = 0, \text{ para casi todo } (i_1, \ldots, i_n) \in \mathbb{N}_0^n \Big\}, \tag{A.4}$$

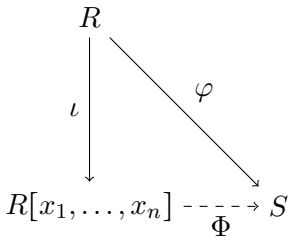
el cual es un anillo conmutativo con elemento identidad.

Sean R y S anillos conmutativos con elemento identidad y $R \subseteq S$. Similar como en el caso de una indeterminada, dado un homomorfismo de anillos $\tau : R \longrightarrow S$ y dados los valores asignados a $x_1, \ldots, x_n$, existe un único homomorfismo $\varphi : R[x_1, \ldots, x_n] \longrightarrow S$ que extiende a τ. También podemos extender el homomorfismo de sustitución.

A.3.2 Teorema. (La propiedad universal) Sean R y S anillos conmutativos y $\varphi : R \longrightarrow S$ un homomorfismo de anillos con $\varphi(1) = 1$ y $s_1, \ldots, s_n \in S$ cualesquiera. Entonces, existe un único homomorfismo

$$\Phi : R[x_1, \ldots, x_n] \longrightarrow S$$

que extiende a φ, es decir, $\Phi\,|_R = \varphi$ y, además, satisface $\Phi(x_j) = s_j$ para $j = 1, \ldots, n$.



Demostración. (1) `Existencia.` La función $\Phi : R[x_1, \ldots, x_n] \longrightarrow S$ definida por

$$\Phi\Big(\sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \Big) = \sum_{i_1, \ldots, i_n \geq 0} \varphi(a_{i_1 \ldots i_n}) s_1^{i_1} \ldots s_n^{i_n}. \tag{A.5}$$

satisface las condiciones exigidas.

Sean $f = \sum a_{i_1\dots i_n} x_1^{i_1}\dots x_n^{i_n}$, $g = \sum b_{j_1\dots j_n} x_1^{j_1}\dots x_n^{j_n} \in K[x_1,\dots,x_n]$. Entonces,

$$\begin{aligned}\Phi(f+g) &= \Phi\Big(\sum (a_{i_1\dots i_n} + b_{j_1\dots j_n}) x_1^{k_1}\dots x_n^{k_n}\Big)\\ &= \sum \varphi(a_{i_1\dots i_n} + b_{j_1\dots j_n}) s_1^{k_1}\dots s_n^{k_n}\\ &= \sum (\varphi(a_{i_1\dots i_n}) + \varphi(b_{j_1\dots j_n})) s_1^{k_1}\dots s_n^{k_n}\\ &= \sum \varphi(a_{i_1\dots i_n}) s_1^{k_1}\dots s_n^{k_n} + \sum \varphi(b_{j_1\dots j_n}) s_1^{k_1}\dots s_n^{k_n}\\ &= \Phi(f) + \Phi(g).\end{aligned}$$

Análogamente,

$$\Phi(fg) = \Phi(f)\Phi(g).$$

Entonces, Φ es un homomorfismo de anillos.

(2) `Unicidad.` Sea $\hat{\Phi} : R[x_1,\dots,x_n] \longrightarrow S$ otro homomorfismo que extiende a φ y que además satisface $\hat{\Phi}(x_j) = s_j$. Entonces,

$$\begin{aligned}\hat{\Phi}\Big(\sum a_{i_1\dots i_n} x_1^{k_1}\dots x_n^{k_n}\Big) &= \sum \hat{\Phi}(a_{i_1\dots i_n})\hat{\Phi}(x_1)^{k_1}\dots\hat{\Phi}(x_n)^{k_n}\\ &= \sum \varphi(a_{i_1\dots i_n}) s_1^{k_1}\dots s_n^{k_n}\\ &= \Phi\Big(\sum a_{i_1\dots i_n} x_1^{k_1}\dots x_n^{k_n}\Big).\end{aligned}$$

En consecuencia, $\hat{\Phi} = \Phi$. □

A.3.3 Teorema. Sean R y S anillos conmutativos con $R \subseteq S$. Entonces para cualesquiera $s_1,\dots,s_n \in S$ la función

$$\Phi : R[x_1,\dots,x_n] \longrightarrow S$$

definida por

$$\Phi\Big(\sum_{i_1,\dots,i_n\geq 0} a_{i_1\dots i_n} x_1^{i_1}\dots x_n^{i_n}\Big) = \sum_{i_1,\dots,i_n\geq 0} a_{i_1\dots i_n} s_1^{i_1}\dots s_n^{i_n} \tag{A.6}$$

es un homomorfismo, el cual se denomina también `homomorfismo de sustitución`.

Demostración. Se deja como ejercicio. □

A.3.4 Corolario. Si R es un dominio entero, entonces:

(1) $R[x_1,\dots,x_n]$ es un domino entero.

(2) $U(R[x_1,\dots,x_n]) = U(R)$.

Demostración. (1) Se deja como ejercicio.

(2) Es una consecuencia del teorema A.1.9. □

ALFABETO GRIEGO

A	α	alpha
B	β	beta
Γ	γ	gamma
Δ	δ	delta
E	ϵ	épsilon
Z	ζ	zeta
E	η	eta
Θ	θ	theta
I	ι	iota
K	κ	kappa
Λ	λ	lambda
M	μ	my
N	ν	ny
Ξ	ξ	xi
O	o	ómicron
Π	π	pi
P	ρ	rho
Σ	σ	sigma
T	τ	tau
Υ	υ	ýpsilon
Φ	ϕ	phi
X	χ	ji
Ψ	ψ	psi
Ω	ω	omega

BIBLIOGRAFÍA

[1] Emil Artin. *Galois Theory*, Lectures Delivered at the University of Notre Dame by (Notre Dame Mathematical Lectures, Number 2), 1997.

[2] Michael Artin. *Algebra*, Pearson; 2 edition, 2010.

[3] Sebastian Castañeda. *Matemáticas fundamentales para estudiantes de ciencias*, Editorial Universidad del Norte, 2017.

[4] L.E. Dickson. *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901; Dover, New York, 1958.

[5] John B. Fraleigh. *A First Course in Abstract Algebra*, Pearson; 7 edition, 2002.

[6] I. Herstein. *Álgebra moderna*, Bogotá Limusa 1967.

[7] John Howie. *Fields and Galois Theory*, Springer - Verlag, 2007.

[8] H. Hungerford. *Algebra*, GTM 73, Springer - Verlag 2003.

[9] Dieter Jungnickel. *Finite Fields: Structure and Arithmetics*, B.I. Wissenschaftsverlag, 1993.

[10] T. Y. Lam. *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Springer - Verlag; 1 edition, 1998.

[11] Serge Lang. *Algebra*, Graduate Texts in Mathematics, Springer - Verlag, 2002.

[12] Rudolph Lidl and Harald Niederreiter. *Introduction to Finite Fields and their Applications*, 2nd Edition, Cambridge University Press, 1994.

[13] Rudolph Lidl and Harald Niederreiter. *Finite Fields*, Volumen 20 de Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1996.

[14] Robert J. McEliece. *Finite Fields for Computer Scientists and Engineers*, The Springer International Series in Engineering and Computer Science, Springer, 1986.

[15] Donald S. Passman. *A Course in Ring Theory*, AMS Chelsea Publishing, 2004.

[16] Steven Roman. *Field Theory*, Graduate Texts in Mathematics, Springer - Verlag, 2nd edition, 2005.

[17] Joseph J. Rotman. *Galois Theory*, Universitext, Springer - Verlag, 1998.

[18] Louis H. Rowen. *Ring Theory*, Student Edition, Academic Press; First Printing edition, 1991.

[19] Zhe-Xian Wan. *Lectures on Finite Fields and Galois Rings*, Beijing, 2003.

ÍNDICE ALFABÉTICO

K-Álgebra, 11
K-automorfismos, 131
U-traza, 136
Álgebra, 11
Álgebra de grupo, 12

Anillo, 2
    de polinomios, 5
    artiniano, 73
    característica de un, 10
    centro, 17
    clases residuales módulo n, 3
    con división, 2
    con elemento identidad, 2
    conmutativo, 2
    cuaterniones, 5
    de factorización única, 61, 63
    de factorización prima, 63
    de ideales principales, 23
    de polinomios, 188
    euclidiano, 28
    factorial, 63
    gaussiano, 63
    localización, 74
    noetherianos, 25
    normado, 55
    primo, 48
    producto cartesiano, 4
    reducido, 71
    series de potencias, 4
Anillo cociente, 22
Anillos
    isomorfos, 30
Automorfismo, 30

Campo, 2
Característica
    de un anillo, 81
Característica de un anillo, 10
Coeficiente binomial, 8
Construcción con regla y compás, 165
Criterio de irreducibilidad de Eisenstein, 58
Cuerpo, 2
    algebraicamente cerrado, 102
    extensión, 84
    extensión algebraica, 91
    extensión cúbica, 85
    extensión cuadrática, 85
    extensión de Galois, 133
    extensión finita, 85
    extensión finitamente generada, 88
    extensión infinita, 85
    extensión inseparable, 125
    extensión normal, 117

extensión separable, 120, 125
extensión simple, 88
extensión trascendente pura, 98
finito, 156
intermedio, 85
la clausura algebraica de un, 100
perfecto, 127
Cuerpo cociente
propiedad universal, 89
Cuerpo fijo de una extensión, 138
Cuerpo finito, 156
extensiones, 161
existencia y unicidad, 157
Cuerpo intermedio, 85
grupo de isotropía de un, 138
Cuerpo primo, 83
Cuerpos de descomposición, 112
existencia, 113

Derivada formal, 120
propiedades, 121
DFU-anillo, 63
División con resto, 190
Divisibilidad, 53
propiedades, 54
Divisor, 53
Divisor de cero, 2
Dominio entero, 2
cuerpo cociente de un, 40
cuerpo de fracciones de un, 41

El teorema fundamental de la teoría de Galois, 131, 140, 163
Elemento algebraico, 90
Elemento idempotente, 70
Elemento identidad, 2
Elemento inseparable, 125
Elemento invertible, 2
Elemento irreducible, 55
Elemento nilpotente, 50
Elemento primo, 55
Elemento separable, 125
Elemento trascendente, 90
Elementos asociados, 53
Elementos construibles, 166
Elementos primitivos
existencia, 130
Elementos primos relativos, 58
Endomorfismo, 30
Epimorfismo, 30
Extensión
elemento primitivo, 88
grado de una, 85
Extensión de Galois, 133
Extensiones algebraicas, 90
Extensiones normales, 117
transitividad, 119
Extensiones separables, 120
transitividad, 129

Fórmula del grado, 86
Frobenius
monomorfismo de, 82
Funciones racionales, 195

Homomorfismo, 30
imagen de un, 32
de sustitución, 192
kernel de un, 32
unitario, 32

Ideal, 18
bilateral, 18
de matrices, 18
derecho, 18
finitamente generado, 23
generado por un conjunto, 23
grado de nilpotencia, 49
intersección, 20
izquierdo, 18
maximal, 45
nil-ideal, 50
nilpotente, 49

primo, 48, 73
principal, 23
producto, 20
propio, 18
suma, 20
trivial, 18
Ideales
del anillo de los enteros, 22
primos, 45
propiedades, 21
Isomorfismo, 30

La clausura algebraica, 100
unicidad, 109
La cuadratura del círculo, 166
La duplicación del cubo, 165
La trisección del ángulo, 166
Lema de Gauss, 65
Lema de Zorn, 46

Matriz escalar, 17
Monomorfismo, 30

Números Gaussianos, 3, 29

Polinomio
cero de un, 192
coeficiente principal de un, 189
cuerpos de descomposición de un, 112
grado de un, 189
inseparable, 123
irreducible, 58
mónico, 189
partición del círculo, 60
primitivo, 58
raíz de un, 192
raíz múltiple, 121
raíz simple, 121
separable, 123
Polinomio minimal, 92
Polinomios, 188
en una indeterminada, 188
sobre DFU-anillos, 64
Potencias, 7
Primer teorema de isomorfía, 36
Propiedad universal, 42, 94, 193
Puntos construibles con regla y compás, 168

Raíz múltiple, 121
Raíz simple, 121

Segundo teorema de isomorfía, 37
Soporte de una sucesión, 185
Soporte finito, 185
Subanillo, 16
generado por un conjunto, 88
trivial, 16
Subcuerpo, 83
generado por un conjunto, 88

Teorema de Artin, 137
Teorema de Cantor, 100
Teorema de correspondencia, 34, 35
Teorema de Gauss, 67, 68
Teorema de Kronecker, 100
Teorema de Krull, 46
Teorema de la base de Hilbert, 27
Teorema de reducción, 60
Teorema de Steiner, 127
Teorema de Steinitz, 104, 115
Teorema de Wilson, 77
Teorema del binomio, 8
Teorema fundamental del álgebra, 102
Tercer teorema de isomorfía, 38
Traza, 136

Unidad, 2
Unidades matriciales, 17

Esta obra, editada en Barranquilla por
Editorial Universidad del Norte en noviembre de 2018.
Se compuso en LaTex.

Este texto, dirigido a estudiantes de pregrado y posgrado en Matemáticas, contiene los temas indispensables en un curso de Álgebra abstracta básica. Está dividido en dos partes: la primera hace énfasis en la teoría de los anillos e incluye generalidades sobre estos, así como homomorfismos de anillos, ideales y algunos tipos especiales de anillos como euclidianos, de factorización única y noetherianos. La segunda parte, dedicada a la teoría de cuerpos, aborda los temas extensiones de cuerpos, una introducción a la teoría de cuerpos finitos y construcciones con regla y compás.

UNIVERSIDAD DEL NORTE